TASK ORDER

47QFCA18F0100 – Modification No. P00023

Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense - Group D (DEFEND D)

in support of:

Department of Homeland Security (DHS)

Issued to:
Booz Allen Hamilton
8283 Greensborough Drive
McLean VA, 22102

Awarded under GSA Alliant Government-wide
Acquisition Contract GS00Q09BGD0019
Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

July 24, 2018
FEDSIM Project Number HS00860

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed. An Acronym List to support this Task Order Request (TOR) is included in **Section J, Attachment B**.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a:

a. Cost-Plus-Award-Fee (CPAF) basis for:
    1. Mandatory CLINs 0001, 1001, 2001, 3001, 4001, and 5001
    2. Optional CLINs 0002, 1002, 2002, 3002, 4002, and 5002
b. Cost-Reimbursable, Not-to-Exceed (NTE) basis for:
    1. CLINs 0003, 1003, 2003, 3003, 4003, and 5003
    2. CLINs 0004, 1004, 2004, 3004, 4004, and 5004
    3. CLINs 0005, 1005, 2005, 3005, 4005, and 5005
    4. CLINs 0006, 1006, 2006, 3006, 4006, and 5006

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from the contractor's facility or assigned location. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.4.1 BASE PERIOD:

MANDATORY LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
0001	Labor (Tasks 1-3)	(b) (4)	[redacted]	$72,688,526

OPTIONAL LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
0002	Labor (Tasks 4-5)	(b) (4)	[redacted]	$15,816,760

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
0003	Long-Distance Travel Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 500,000
0004	Tools Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$50,774,852
0005	ODCs Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 5,000,000

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
0006	Contract Access Fee	NTE	$ 100,000

TOTAL BASE PERIOD CLINs: **$ 144,880,138**

B.4.2 FIRST OPTION PERIOD

MANDATORY LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
1001	Labor (Tasks 1-3)	(b) (4)	(b) (4)	$95,923,048

OPTIONAL LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
1002	Labor (Tasks 4-5)	(b) (4)	(b) (4)	$20,364,025

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
1003	Long-Distance Travel Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 500,000
1004	Tools Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 55,006,090
1005	ODCs Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 5,000,000

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
1006	Contract Access Fee	NTE	$ 100,000

TOTAL FIRST OPTION PERIOD CLINs: $ 176,893,163

B.4.3 SECOND OPTION PERIOD

MANDATORY LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
2001	Labor (Tasks 1-3)	(b) (4)	(b) (4)	$96,499,881

OPTIONAL LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
2002	Labor (Tasks 4-5)	(b) (4)	(b) (4)	$21,154,189

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
2003	Long-Distance Travel Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 500,000
2004	Tools Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 59,237,327
2005	ODCs Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	$ 5,000,000

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
2006	Contract Access Fee	NTE	$ 100,000

TOTAL SECOND OPTION PERIOD CLINs: $ 182,491,397

B.4.4 THIRD OPTION PERIOD

MANDATORY LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
3001	Labor (Tasks 1-3)	(b) (4)	(b) (4)	(b) (4)

OPTIONAL LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
3002	Labor (Tasks 4-5)	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
3003	Long-Distance Travel Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)
3004	Tools Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)
3005	ODCs Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
3006	Contract Access Fee	NTE	(b) (4)

TOTAL THIRD OPTION PERIOD CLINs: (b) (4)

B.4.5 FOURTH OPTION PERIOD

MANDATORY LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
4001	Labor (Tasks 1-3)	(b) (4)		

OPTIONAL LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
4002	Labor (Tasks 4-5)	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
4003	Long-Distance Travel Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)
4004	Tools Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)
4005	ODCs Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
4006	Contract Access Fee	NTE	(b) (4)

TOTAL FOURTH OPTION PERIOD CLINs: (b) (4)

B.4.6 FIFTH OPTION PERIOD

MANDATORY LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
5001	Labor (Tasks 1-3)	(b) (4)		

OPTIONAL LABOR CLIN (CPAF)

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
5002	Labor (Tasks 4-5)	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
5003	Long-Distance Travel Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)
5004	Tools Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)
5005	ODCs Including Indirect Handling Rate G&A (b) (4) and MH (b) (4)	NTE	(b) (4)

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
5006	Contract Access Fee	NTE	(b) (4)

TOTAL FIFTH OPTION PERIOD CLINs: (b) (4)

GRAND TOTAL ALL CLINs: **$ 1,036,581,961**

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

All proposed labor categories shall be mapped to existing Alliant labor categories.

B.6 INCREMENTAL FUNDING

B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of **$137,436,506.26 for CLINs 0001, 0002, 0003, 0004, 0005, 0006, 1001, 1002, 1003, 1004, and 1006** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated Period of Performance (POP) covered by the allotments for the mandatory **CLINs 0001, 0002, 0003, 0004, 0005, and 0006** is from award through **August 5, 2019**, and for mandatory **CLINs 1001, 1002, 1003, 1004, and 1006** is from **August 6, 2019** through **February 29, 2020**, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of **$1,036,581,961** over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

B.6.1.2 INCREMENTAL FUNDING CHART FOR CPAF

See **Section J, Attachment G** - Incremental Funding Chart.

B.7 AWARD FEE PLANNED VALUE/RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) documents the award fee. See **Section J, Attachment E**.

C.1 BACKGROUND

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. As threats to the nation's information security continue to emerge, Government leaders recognize the need for a modified approach to protecting the Government's cyber infrastructure. The CDM Program enables the Department of Homeland Security (DHS), Federal Agencies, and state, local, regional, and tribal governments to enhance and further automate their existing continuous network monitoring capabilities, compare and analyze critical cybersecurity-related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating Agencies by helping to identify information security risks on an ongoing basis so that Agencies can rapidly detect and then respond to information security events.

Congress established the CDM Program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. The CDM Program provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Starting in January 2013, DHS (operating on behalf of the participating Agencies) provided tools/sensors and services to execute Phase 1 of the CDM Program, which implemented the CDM Solution at each Agency in this TO. Beginning in June 2016, DHS provided tools/sensors and services to participating Agencies to execute Phase 2 of the CDM Program.

The CDM Program is organized by phases as identified below in Diagram 1: CDM Phases.

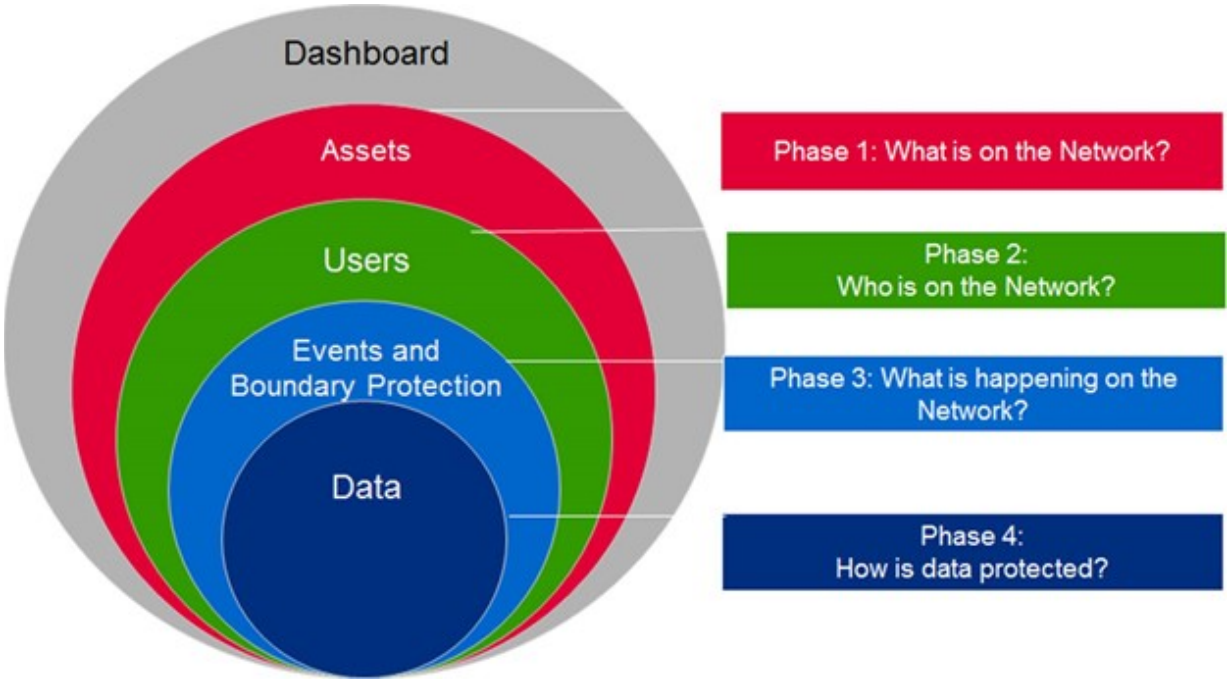

Diagram 1: CDM Phases

C.1.1 PURPOSE

The purpose of this TO is to resolve CDM capability gaps, enhance existing CDM capabilities, introduce new CDM capabilities, and provide support to the CDM Solution of participating Agencies, leading to a strengthening of their overall cybersecurity posture. The CDM Solution includes CDM-approved products, configured to reflect the DHS CDM Program priorities and Agency policies as appropriate, that implement a common set of capabilities and enable increased risk-reduction and alignment with Agency risk tolerance.

C.1.2 DHS CDM PROGRAM MISSION

The CDM Program is managed within the DHS National Protection and Programs Directorate, (NPPD)/Office of Cybersecurity and Communications (CS&C)/Network Security Deployment (NSD) Division, responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. The DHS CDM Program mission is to safeguard and secure cyberspace in an environment where the threat of cyber-attack is continuously growing and evolving. The CDM Program defends the United States (U.S.) Federal Information Technology (IT) networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. DHS has been given the authority and Federal funding to implement the CDM Program to ensure that the approach to continuous monitoring is consistent, meets a common set of capabilities, and leverages centralized acquisition to improve the speed of procurement and achieve significant cost savings by consolidating like Federal requirements into "buying groups." This TO is intended to achieve those objectives.

C.2 SCOPE

The scope of this TO is to provide support for all phases of the CDM Program and implement a common set of CDM capabilities across Federal Agencies. Within scope of this TO, the contractor will be required to:

a. Provision Agencies with CDM-approved products, support ancillary products, and provide the associated services to the participating Agencies.
b. Fill existing gaps in Agency CDM Solutions to achieve a common set of capabilities.
c. Provide Operations and Maintenance Support (O&M) to the existing CDM Solution, while continuing to enhance and refresh CDM-approved products, as appropriate.
d. Plan for Agency support of provisioning, configuring, operating, testing, and managing CDM tools, sensors, Agency-level dashboards, and data feeds as well as support for the CDM Solution's governance.
e. Develop, integrate, operate, and maintain the capability for CDM-approved products to report information to the Agency-level CDM Agency Dashboard.
f. Design, build, deploy, and operate the CDM Solution for component offices of the participating Agencies that opt into the CDM Program.
g. Provide Agency-specific training for the CDM Solution, the Agency CDM Dashboard, and CDM governance support.

The performance of this TO is primarily at the contractor's facility; however, testing and validation efforts may require performance at Government facilities. The contractor's facility shall include spaces suitable for a development and test facility and support classified IT storage.

C.2.1 Supported Agencies

This TO will support the DHS CDM Program Management Office (PMO) by providing and/or enhancing the CDM Solution at the following Federal Agencies and their components, hereafter referred to as the Group D Agencies:

a. The United States General Services Administration (GSA)

b. The United States Department of Health and Human Services (HHS)

c. The United States National Aeronautics and Space Administration (NASA)

d. The United States Social Security Administration (SSA)

e. The United States Department of Treasury (Treasury)

f. The United States Postal Service (USPS)

C.3 OBJECTIVES

The objective of this TO is to operate and enhance the existing Group D CDM Solution. In compliance with applicable standards, this objective will be accomplished through detection improvement and analysis of IT security events and in cooperation with the DHS CDM PMO and the Group D end users.

Additional CDM Program objectives for the TO are to:

a. Reduce Agency threat surface through strengthening cybersecurity of Agency IT assets.
b. Achieve the most advantageous cost and price discounts while provisioning Agencies with CDM tools and capabilities.
c. Deliver flexible services that can accommodate dynamic cyber environments.
d. Timely completion of work to ensure delivered CDM capabilities are fully implemented at receiving Agencies.
e. Promote transparent and effective communications that accurately present status to CDM stakeholders.
f. Provide accurate reporting of Agency environments while achieving successful governance of Agency cybersecurity programs.

C.4 CDM CURRENT AND FUTURE STATES

CDM enables activities designed to strengthen the cybersecurity posture of the Federal civilian .gov networks. Specifically, the tools and sensors and associated services benefit the CDM Program by:

a. Simplifying the security authorization process by helping to automate security assessments.
b. Monitoring and reporting continuous system security status to Agency cybersecurity personnel via the Agency CDM Dashboard.

c. Providing specific details to help prioritize remediation efforts.
d. Allowing system owners, risk managers, authorizing officials, and other stakeholders to make better risk-management decisions.
e. Automating reporting of the security posture of Agency IT assets to the Federal Dashboard, thereby reducing the requirement for manual reporting.

The remainder of **Section C.4** summarizes the CDM Current State, CDM Desired Future State, and CDM Technical Capabilities. Where there is a perceived conflict between **Section C.4** and the CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**), the CDM Technical Capabilities Requirements Documents will take precedence.

C.4.1 CDM CURRENT STATE

An Agency-specific CDM Solution is currently operating on the Agencies' networks with diverse IT environments. The CDM Solution maintains a degree of consistency across the Group D Agencies by leveraging a similar set of Commercial Off-the-Shelf (COTS) tools. These tools have been reviewed by the DHS CDM PMO to identify that they meet the capabilities of, or in conjunction meet, the requirements specified in CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**). A list of approved CDM tools is maintained by the DHS CDM PMO as the Approved Product List (APL) and is located at www.gsa.gov/CDM.

CDM approved and supportingancillary products currently in use at the Agencies, as well as high-level IT and network infrastructure descriptions for each Agency supported by this TO, are identified in the Agency-specific IT/Network Environment Summary Information provided by the Government in the Electronic Reading Room (eRR). The Government desires that the contractor leverage any existing Agency investments when developing a solution for any CDM capability enhancement or new integration.

Initial Support for USPS under Task 1, Task 2 and Task 3 will be executed through post-award RFS in accordance with **Section C.5**. USPS support will not begin immediately at Project Start.

The CDM system architecture, shown below in **Diagram 2** – CDM Architecture, illustrates the CDM Full Operating Capabilities (FOC) vision once it has been implemented within the Group D Agencies.

a. Area A is the location for tools and sensors that, together, provide the coverage of the CDM capabilities.
b. Area B is the integration point solution that supports the required operational control points for the CDM Solution.
c. Area C is the Agency CDM Dashboard(s) that integrates into the Agency CDM Solution.
d. Area D is the Federal CDM Dashboard.

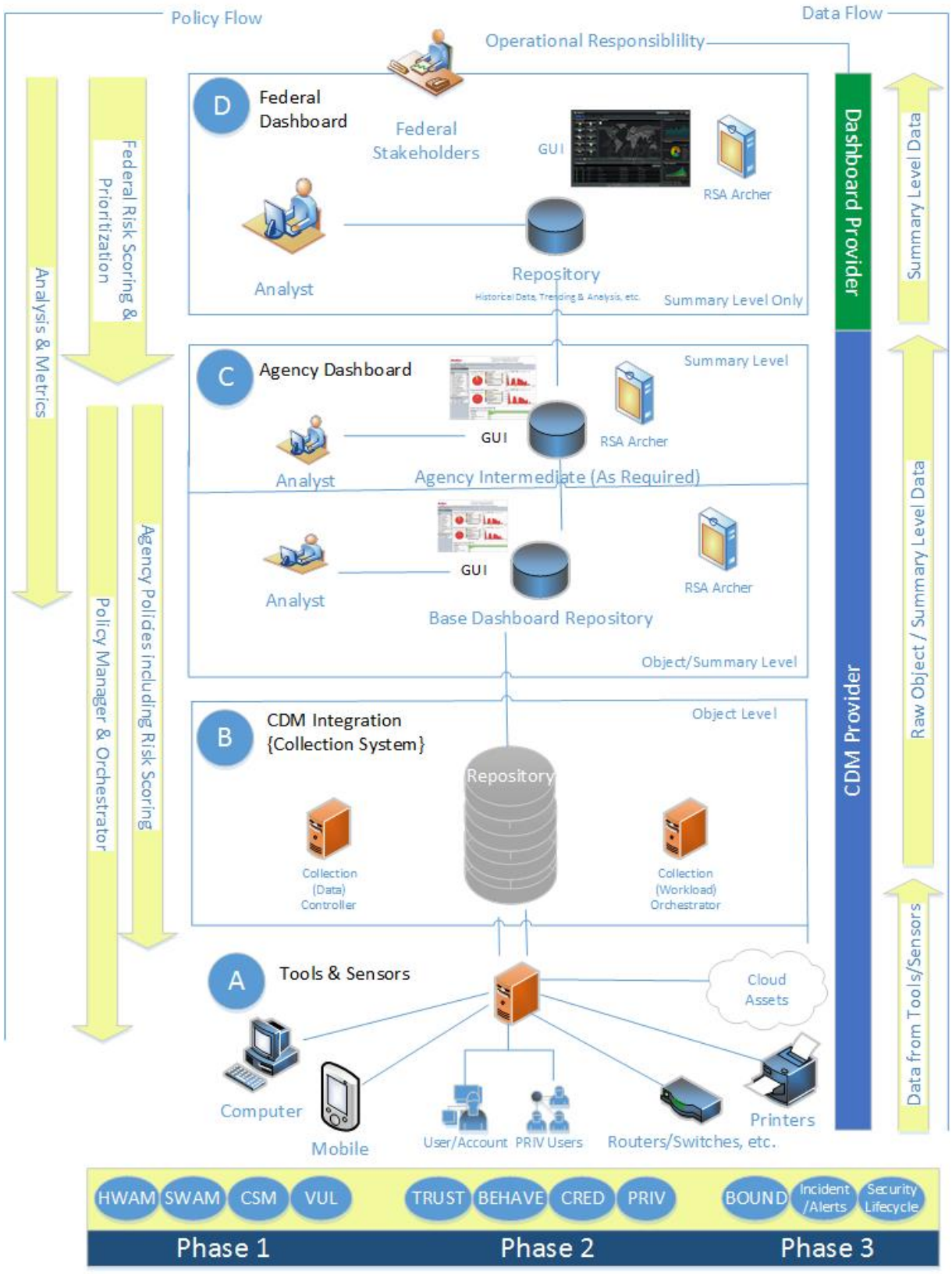

Diagram 2: CDM Architecture

C.4.2 CDM DESIRED FUTURE STATE

The CDM Solution at each Agency shall meet the operational and functional requirements as detailed in CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**) for all CDM areas.

The Government requires an integrated solution that includes support for each Phase of the CDM Program. This multi-phase integrated solution will provide a common set of capabilities across the Agencies to fulfill the capabilities of the four phases of the CDM Program. The Government desires continued enhancement of data aggregation for the Agency Dashboards, then integration through the Federal Dashboard to improve the visibility and identification of cyber threats to Federal Networks. In support of the existing CDM Solution, the contractor shall sustain an integration layer to the Agency and Federal Dashboards, update the Agency Dashboard releases, and integrate the Phase 1 and Phase 2 capabilities. Maintaining the current CDM Solution is not merely continuing a steady state. It requires flexibility, agility, and responsiveness to the evolving cyber threats facing Government networks.

The proposed CDM Solution shall leverage, to the maximum extent possible, modern practices and COTS technology to iteratively develop and deploy an integrated CDM Solution.

The CDM Solution shall be designed and developed, first and foremost, with the Agencies and their end users' experience in mind. The contractor's proposed CDM Solution shall advance the CDM Program's objective to provide a common set of capabilities, but be configured and tailored for DHS needs to provide easy access to the appropriate workflows, tools, reports, and data. The user solutions shall be designed in a way that is easy to use so as to reduce the need for system training.

Given the criticality of the CDM mission, the CDM Solution shall:

a. Meet or exceed industry standards for system availability.
b. Secure certain data in a way that ensures it can be seen and accessed only by those with a "need to know."
c. Integrate seamlessly with all legacy applications and external partners and not cause any disruption to mission-essential Agency systems and networks.

The CDM Solution shall allow the data to be aggregated and cleaned to support data analytics and reporting needs without adversely impacting the performance of transactional systems/applications.

Due to rigid governance structures, diversity of mission, and the interconnectedness of the Agencies' environments, most Agencies have yet to develop an enterprise-class IT solution using modern system development practices. Regardless, the CDM Program has a strong preference for utilizing modern development methodologies including, but not limited to, Agile Scrum, Kanban, or Scaled Agile Framework (SAFe).

CDM tools and sensors will need to be refreshed as appropriate. The CDM Solution shall provide continued integration, operation, and maintenance of the Agency-level CDM Dashboard ensuring that all installed CDM tools and sensors report to the Agency Dashboard as necessary. The Government recognizes that many of the CDM tools and sensors are able to meet multiple phase capabilities; therefore, any solution must, to the maximum extent possible and practicable, build off of the existing CDM investments. The CDM program requires improved support to

identify efficiencies and cost savings, as well as track progress and deployment schedules across the Agencies.

C.4.3 CDM TECHNICAL CAPABILITIES

The CDM Program is organized by phases, which are not necessarily sequential, and the Government may require the contractor to provide support on multiple phases in parallel. Each CDM phase consists of multiple CDM capabilities, which are summarized in the following sections. The detailed functional and operational requirements of the capability areas can be found in the CDM Technical Capabilities Requirements Document, Volume 2 (**Section J, Attachment Y.2**). The Government desires that the contractor leverage existing Agency investments when developing solutions for CDM capabilities. The contractor shall provide support to the **Section C.6** Tasks to accomplish the following:

C.4.3.1 MANAGE "WHAT IS ON THE NETWORK"

CDM Phase 1 requires the contractor to acquire, deploy, and maintain CDM-approved products that support the CDM Program Phase 1 capabilities (i.e., Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Setting Management (CSM), and Vulnerability Management (VUL)).

The focus of CDM Phase 1 is to manage assets by identifying "what is on the network." Specifically, this includes identifying the existence of hardware, software, configuration characteristics, and known security vulnerabilities. HWAM and SWAM cover verification and validation for the existence of hardware devices and the accurate identification of approved software components. CSM covers the verification and validation that hardware devices have the correct security configuration settings, and the system platform is hardened to reduce the platform attack surface. VUL covers verification and validation of preventing and detecting software vulnerabilities to measure software assurance for built and acquired software components.

Each Agency in this TO has made Phase 1 investments, and the contractor shall identify and fill any existing gaps in Phase 1 functionality. This TO expands the CDM Phase 1 functionality to assets that were not previously covered; these are identified in **Table 1: CDM Phase 1 Capabilities**.

Table 1: CDM Phase 1 Capabilities

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
CDM Phase 1		
HWAM	End point (Workstations, Servers) Network Devices (infrastructure) IP addressable assets	Mobile Devices and Mobile Device Manager (MDM) (h) Cloud-Based Assets (g)

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
CDM Phase 1		
SWAM	Operating System (a) Common Applications (b) Other Applications (c) Application Integrity (e.g., Whitelisting) (d)	Mobile Devices (h) Cloud-Based Assets (g) Code Validation (e)
CSM	Operating System (a) Common Applications (b)	Mobile Devices (h) Cloud-Based Assets (g) Database (DB)/Web Common Weakness Enumerations (CWEs) (f)
VUL	Operating System (a) Common Applications (b)	Mobile Devices(h) Cloud-Based Assets (g) DB/Web CWEs (f)

The following defines the assets identified in **Table 1**:

a. Operating System - As defined in the National Vulnerability Database (NVD) product category of "Operating System" within the Common Platform Enumerations (CPEs).

b. Common Applications - Generally defined in NVD as not "Operating System," to include categories as "desktop application" or "database management" for the CPE.

c. Other Applications - Software that does not have identification within NVD (SWAM).

d. Application Integrity - The part of SWAM that assures the asset identified is a correct and proper instance and is fully authorized. This is usually done through a whitelisting tool and method (SWAM).

e. Code Validation - The part of SWAM that assures the code used to create applications does not contain vulnerabilities.

f. DB/Web CWEs - This is for products specifically designed to manage Database/Web vulnerabilities or configuration settings and reporting in the form of CWEs versus Common Vulnerability Enumerations (CVEs).

g. Cloud Assets - As defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

h. Mobile Devices and MDM - Mobile device scope will include integration services with existing Agency MDM solutions and the extent to which the MDM is compliant with Agency defined MDM security benchmark. As defined in NIST SP 800-124 Rev 1 (or

most current version), “The following hardware and software characteristics collectively define the baseline of mobile devices:

1. A small form factor.
2. At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the internet or other data networks.
3. Local built-in (non-removable) data storage.
4. An operating system that is not a full-fledged desktop or laptop operating system.
5. Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties).”

The expansion of CDM capabilities to Agency cloud and mobile environments are addressed in the two following sections.

C.4.3.1.1 COVERAGE OF CLOUD ASSETS

The approach to expanding CDM capabilities to Agency cloud environments requires that the cloud be viewed as two distinct ecosystems. In the first cloud ecosystem, an Agency has identifiable assets that would appear as extensions to the Agency’s on premise ecosystem (this could be viewed as a private Infrastructure as a Service (IaaS)). In this scenario, the standard CDM architecture that is used for an on premise CDM Solution shall be extrapolated to cloud assets.

In the second cloud ecosystem, full transparency to assets is not available, such as in a shared service, and/or the mechanism used in defining the relationship between the Cloud Service Provider (CSP) and Agency. In this cloud ecosystem, only the applicable tracking of CDM metrics applies, which in general is information provided within the Federal Risk and Authorization Management Program (FEDRAMP) process and agreements. Major items (several of which are beyond the Phase 1 requirements) that need to be conveyed to the Agency from the CSP would include:

a. Vulnerabilities of concern to the Agency.
b. Incident response interactions.
c. Method of control assessment to integrate to the Agency’s ongoing assessment/authorization.
d. Processes/mechanisms for supporting the Government’s post-incident forensics activities.
e. Enterprise account hijacking as it pertains to Agency virtual environment(s).
f. Availability and support of Application Programming Interface (API) for Agencies to automate the extraction of necessary logs that provides situational awareness (e.g., netflow, user access, etc.).
g. Integration of security logs into the Agency security toolsets.
h. CSP approach to data deletion.
i. CSP Ability to mitigate Distributed Denial of Service (DDOS) attacks.
j. Disclosure of malicious provisioning of CSP enterprise resources to Agency customers.

The second cloud ecosystem will require identification of a connection mechanism to the CSP service data source and establish a work flow to provide this information to the Agency's CDM Solution and ultimately to the CDM Dashboard. The development of this connection mechanism will address all requirements of CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**), unless otherwise noted, in which case a rationale for exclusion will be provided. For example, in Phase 1, only VUL requirements may be addressed since HWAM, SWAM, and CM are not under the control of the Agency.

C.4.3.1.2 COVERAGE OF MOBILE ASSETS

The Agencies supported in this TO are expected to establish and deploy an enterprise mobile solution, like an MDM, that will support mobile asset reporting and policy control. Establishing an MDM and providing any related infrastructure are not within the scope of this TO and are planned to be provided by the Agency. Further, configuring an existing Agency MDM according to security benchmarks is not planned to be within the scope of this TO. CDM data will be integrated from existing Agency mobile solutions, such as an MDM, into the Agency's CDM Solution. To accomplish this, both a data exchange mechanism to an Agency-deployed MDM (or similar mobile enterprise solution) and a work flow to provide this information to the Agency's CDM Solution, and ultimately to the CDM Agency Dashboard, will be required.

C.4.3.2 MANAGE "WHO IS ON THE NETWORK"

CDM Phase 2 requires the contractor to acquire and deploy CDM-approved products that support the CDM Phase 2 capabilities (TRUST, BEHAVE, CRED, and PRIV).

The focus of CDM Phase 2 is to determine "who is on the network." Specifically, this includes identifying and determining the users or systems with access authorization, authenticated permissions, and granted resource rights. The CDM Phase 2 capabilities collectively cover the verification and validation of allowed user privileges, user-owned credentials, user security behavior training, and appropriately granted resource access rights to users.

Each Agency in this TO has made or is in the process of making Phase 2 investments, and the contractor will identify and fill any existing gaps in Phase 2 functionality. This TO expands CDM Phase 2 functionality to assets that were not previously covered, and are identified in **Table 2: CDM Phase 2 Capabilities**.

Table 2: CDM Phase 2 Capabilities

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
CDM Phase 2		
TRUST	Agency Users/Accounts	Accounts for Cloud/Mobile Assets
BEHAVE	Agency Users/Accounts	Accounts for Cloud/Mobile Assets
CRED	Agency Users/Accounts	Accounts for Cloud/Mobile Assets

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
PRIV	Agency Users/Accounts	Accounts for Cloud/Mobile Assets

In **Table 2**, the following definitions apply:

User - A generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

Account - The means by which a user can access a system.

C.4.3.3 MANAGE "WHAT IS HAPPENING ON THE NETWORK AND HOW IS THE NETWORK PROTECTED"

CDM Phase 3 requires the contractor to acquire and deploy CDM-approved products that support the CDM Program Phase 3 capability areas of Manage Events (MNGEVT); Operate, Monitor, and Improve (OMI); Design and Build in Security (DBS); and Boundary Protection (BOUND).

MNGEVT is preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through data analysis. MNGEVT covers verification and validation of processes, policies, and procedures supporting cybersecurity preparation, audit and log data collection, security analysis of audit/log data, and incident reporting to provide forensic evidence of malicious or suspicious behavior (**Section J, Attachment Y.2**, Section II – 4.2).

OMI includes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing). OMI covers verification and validation of processes/procedures to prioritize incidents and associated response actions, to quickly mitigate the impact of an incident, take appropriate remediation actions to eliminate the impact (restore normal operations) of the same incident, and to support information sharing and collaboration (both internal and external) to minimize or prevent the impact of future incidents (**Section J, Attachment Y.2**, Section II – 4.3).

DBS is preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment. The DBS process is focused on identifying, controlling, and removing weaknesses/vulnerabilities from the software/system. Exploitable vulnerabilities may include software/system design, coding errors, software/system designs that leave a large and complex attack surface that cannot be defended and weaknesses that can only be exploited during system/software execution. DBS covers verification and validation of preventing and detecting software vulnerabilities to measure software assurance for built and acquired software components (**Section J, Attachment Y.2**, Section II – 4.4).

The focus of BOUND is to provide boundary protection for the interior of the network from all interconnections to other external networks. Specifically, it is the determination of the user/system actions and behavior at the network boundaries and within the computing infrastructure. BOUND covers verification and validation of logical and physical network interfaces to reduce intrusive, malicious, and disruptive attacks, cryptographic mechanisms to

ensure confidentiality and integrity of data on the network, and methods to identify security incidents (**Section J, Attachment Y.2**, Section II – 4.1).

The following sections (**C.4.3.3.1** through **C.4.3.3.8**) summarize CDM Phase 3 capabilities that represent a new CDM area of capabilities for the Group D Agencies.

C.4.3.3.1 INCIDENT RESPONSE AUTOMATION

Incident response automation is the orchestration that is necessary to support the respond function with automated tools to the maximum extent possible. Orchestration to support the respond function is focused on providing tools and sensors that provide the following functionalities:

a. Incident response event notification.
b. Incident handling data collection.
c. Incident monitoring.
d. Incident reporting.
e. Incident response devices.

These capabilities are focused on the aspects of the incident handling process, rather than the aspects of reporting the incident response activities. In each of these capabilities, the focus is on being able to collect and correlate data, analyze the data, and provide notifications to the incident response staff. This capability includes the ability to automate the incident response process, where possible, to include the following functionalities:

a. Scanning for recognition of malicious content.
b. Automated malware analysis tools.
c. Aggregation of threat intelligence data.

Incident response automation (including response) will be focused on collating and condensing relevant information for intelligent decision making that ultimately facilitates positive discovery and reporting of incidents, subject to CDM guidance. The contractor shall work with existing Security Operation Center (SOC) assets under this capability area to provide a holistic solution that achieves the results provided in the CDM Technical Capabilities Requirements Documents (**Section J, Attachments Y.1 and Y.2**).

C.4.3.3.2 ONGOING ASSESSMENT

The Government requires a capability to help achieve greater automation, accuracy, and frequency related to the implementation status of Agency's associated NIST 800-53 controls (most current version) and Agency-defined parameters. The current, relatively labor-intensive process of conducting NIST 800-53a security assessments offers the CDM Program an opportunity to enable significant efficiencies, cost-savings, and increased data quality by incorporating existing CDM data and technologies with new capabilities.

Ongoing assessment relates the existing Agency Dashboard object and/or summary information to an Agency's associated NIST SP 800-53 controls as defined and implemented so that each Agency's posture is continuously automated for Agency authorization decisions relative to their stated risk tolerance.

The objective of ongoing assessment is the continuous assessment of Agency security and privacy policies related to static object attributes (i.e., actual state and desired state) for threat behaviors which impact the security and privacy posture of an Agency's existing NIST SP 800-53 controls and countermeasures. Ongoing assessment also encompasses the identification of new component weaknesses and vulnerabilities that represent unauthorized deviations to an Agency.

C.4.3.3.3 ONGOING AUTHORIZATION

The Government has a need to improve the efficiency, data quality, and currency and reduce cost related to current security authorization processes.

Ongoing authorization uses the results of the ongoing assessment of NIST SP 800-53 controls for all previous phases of CDM as a set of inputs for the orchestration of ongoing authorization, risk assessment, and acceptance processes. These processes support and orchestrate with the needs of Agency personnel assigned to oversee Agency risk tolerance in accordance with the status of the required NIST 800-53r4 controls and Agency-specific parameters.

Ongoing authorization allows Agencies, senior risk management, and cybersecurity personnel the ability to quickly assess security risk against acceptable security risk levels and adjust security requirements or NIST SP 800-53 controls and countermeasures to ensure that an acceptable level of security risk is maintained. This approach is much more efficient than the traditional multiyear security assessment and authorization methods with which Agencies maintain and accept residual risk.

Ongoing authorization provides the ability to automate the determination and necessary updates to NIST 800-53 controls and countermeasures, to allow systems to be evaluated and authorized when CDM system changes are made, or automate Plan of Action and Milestone (POA&M) creation when security controls are identified as not maintaining risk at approved levels as defined by Agencies.

C.4.3.3.4 BOUND FILTERING BY NETWORK

The BOUND function provides Agencies with visibility into the risk associated with connections or access to networks, systems, and data. To provide this visibility, BOUND Filtering (BOUND-F) (also referred to as Manage Network Filters and Boundary Controls) by Network utilizes filters that include devices like firewalls and gateways that sit at the boundary between enclaves, such as a trusted internal network or subnet and an external or internal, less-trusted network. The Government considers an enclave as a collection of information systems connected by one or more internal networks under the control of a single authority and security policy, with the systems being structured by physical proximity or by function, independent of location.

The filters apply sets of rules and heuristics to regulate the flow of traffic between the trusted and less trusted sides based on network attributes (such as ports and protocols). The overall objective of BOUND-F is to reduce the probability that unauthorized traffic passes through a network boundary.

This BOUND-F functionality provides an analysis of an Agency's existing network-based filtering capabilities and improves and augments this protection for an Agency. Additionally, it

includes the ability to examine encrypted content if possible. The types of network devices/capabilities that are encompassed by BOUND-F include, but are not limited to:

a. Packet filtering
b. Proxies
c. Network access protection
d. Encapsulation Filtering
e. Also included would be:
    1. Internet for Federal Government:
        i. EINSTEIN
        ii. Trusted Internet Connection (TIC)

BOUND-F requires that boundary policies include monitoring, reviewing, and reauthorizing consistent with any Agency policy. In addition, BOUND-F allows for the reporting of the effectiveness of the detect/protect characteristics of these technical elements as well as relevant asset information are also required.

C.4.3.3.5 BOUND FILTERING BY CONTENT

Content-based perimeter protection prevents unwanted content from entering or leaving the gateway of a network. BOUND-F content filtering examines network traffic at the application level to block or filter malware or prohibited traffic from entering or leaving the network. The two common areas of content filtering are web (Hypertext Transfer Protocol (HTTP) and email Simple Mail Transfer Protocol (SMTP). Web content filter includes protecting servers from common web attacks by using a Web Application Firewall (WAF) to inspect HTTP traffic. Web Malware protection is used to inspect web traffic for malicious code and block it before it can reach endpoints in the Agency network. Web content filters block Agency endpoints from reaching prohibited websites and Internet Protocol (IP) addresses. Email content filtering uses message content such as attachments, headers, or content in the message body, to block an email based on Agency policies. Email content filtering can also provide anti-phishing capabilities. Email malware protection inspects and analyzes email traffic for malicious content and blocks or prevents its spread.

BOUND-F filtering by content provides an analysis of an Agency's existing web and email content filtering capabilities and improves and fills in content filtering protection for an Agency. Capabilities include the ability to examine encrypted content where appropriate. In addition, BOUND-F filtering by content allows for the reporting of the effectiveness of the detect/protect characteristics of these technical elements as well as relevant asset information.

C.4.3.3.6 DATA-BASED PERIMETER PROTECTION

The DBS function of data-based perimeter protection focuses on the identification and prevention of data exfiltration within the Agency. Data-based perimeter protection is a broad category of protections that includes the technologies used for Data Leak/Loss Prevention (DLP). This protection provides the capability to mitigate the effects of insider threat activities to include, but not limited to, the following:

a. Manipulating files without authorization.

b. Printing protected data.
c. Exporting protected data outside of the Agency.
d. Intercepting protected data as it transits to the Agency network.

The technologies to implement this type of protection typically focus on the inspection of packets as they move across the network with the objective of identifying potential data movement attempts. These technologies can also include the use of device-based diagnostics to recognize unusual activities involving the protected data. This protection can be in the form of blocking, monitoring, or notification when a suspected data loss event is in progress.

C.4.3.3.7 BOUND-ENCRYPTION

Cryptographic mechanisms protect credentials, data at rest, and data in motion. An identity credential is a digital representation of a user. The identity credentials are often implemented on an integrated circuit smart card, in particular the Federal Personal Identity Verification (PIV) card as specified in Federal Information Processing Standards (FIPS)-201-2. FIPS 201 credentials commonly include information such as private keys, pins, digital certificates, and encoded biometric values. Credentials are used to authenticate users, systems, software packages and other resources in the system. Data at rest protection includes encryption of individual files, as well as encryption of entire volumes/disks. Components of data at rest encryption include both the encryption software itself and the encrypted data. Data in motion cryptography involves the use of application security protocols such as Secure/Multipurpose Internet Mail Extensions (S/MIME) and Secure Shell (SSH); web-based transactions using Secure Sockets Layer (SSL)/Transport Layer Security (TLS); and Virtual Private Networks (VPNs) using Internet Protocol Security (IPsec) and SSL/TLS.

Together these cryptographic techniques and related cryptographic keys/credentials provide critical security functions to support the confidentiality, integrity and authenticity of network functions both internally to protect insider threats and externally to prevent malicious behaviors.

Boundary Encryption (BOUND-E) functionality provides indications of improper cryptographic behavior and/or hardware/software misconfiguration on Agency Assets. Cryptography must be properly implemented and configured in order to provide the desired level of protection. Support of BOUND-E provides Agencies with capabilities to collect policies from hardware device, software product, and cryptographic implementation configuration settings, to ensure that the right implementations are being used and configured properly. In addition, support of BOUND-E provides capabilities to manage and monitor cryptographic key management systems.

Targeted Capabilities include, but are not limited to, the following:

a. Ability to monitor public key Certificate Authority compliance with the Federal Root Certificate Policy Authority.
b. Ability to monitor PIV card compliance with FIPS 201-2 Key Management and Cardholder Authentication requirements.
c. Ability to collect as-is state data elements and attributes and compare with desired state attributes per the CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**).

C.4.3.3.8 INCORPORATION OF SYSTEM ASSURANCE (SOFTWARE/HARDWARE)

Improving Agency capabilities with respect to secure systems engineering development is well understood to be a best practice and one that readily reduces cost and risk to IT projects. This is the implementation of the requirements identified as the design/build-in security capability. Supporting system assurance reduces the attack surface for network and infrastructure components during acquisition, development, and deployment and reduces project costs associated with poor security engineering practices.

The following DBS capabilities support this goal:

a. Supply Chain Risk Management (SCRM) attributes.
b. Software development assurance (code inspection/analysis).
c. Application weakness detection (web-based vulnerabilities such as CWE and secure configuration, as well as database focused).

Supply Chain Risk Management (SCRM)

The purpose of SCRM is to enable the provisioning of the least vulnerable solutions to Agencies, through a robust assessment of supply chain risks, communication of those risks to the Agencies, and the appropriate response and monitoring of those risks throughout the entire system life. SCRM impacts this TO in two distinct ways. First, the contractor shall apply best SCRM practices (to include any teaming partners or vendors) within the execution of the TO. The second SCRM impact is through the contractor assisting Agencies to establish continuous improvement (to include measurable outcomes) within the Group D Agencies in terms of Agency-specific governance.

Software Development Assurance (code inspection/analysis)

Software development assurance introduces the ability to develop secure code via code inspection and to use security testing and evaluation during development, such as those prescribed by the NIST 800-53r4 control, SA-11 Developer Security Testing and Evaluation. Software development assurance also assists Agencies in ensuring that security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements as modeled after production configurations. Security testing and evaluation includes flaw remediation/correction processes, static code analysis, other types of analysis and reviews, and testing artifacts.

Software development assurance also includes increasing scope of existing CDM tools from Phase 1 into development enclaves and network boundaries, such that production machine-level desired states are integrated into development efforts to ensure continuity of configurations.

Application Weakness Detection

During deployment and operation, runtime software systems continuously assess and monitor for vulnerabilities and exploits of software weaknesses, in designated Agency networks, to the maximum extent possible. Dynamic assessment tools are utilized to support general software assurance needs in both development and production scenarios, where possible, and tailored to address availability and performance concerns.

In addition, the operating system platform shall be monitored for malicious attacks on the weaknesses and vulnerabilities of the operating system, platform tools, and utilities.

C.4.3.4 MANAGE "HOW DATA IS PROTECTED ON THE NETWORK"

CDM Phase 4 capabilities described below support the overall CDM Program goals to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These fundamental requirements may be accomplished in new and innovative methods that transcend the current CDM architecture model. The following sections are examples of portions of the solutions that could be associated with protecting data on the Agencies' networks.

C.4.3.4.1 MICRO-SEGMENTATION

Micro-segmentation is the virtualization of the data center or a cloud computing structure. It is a security technique that integrates security directly into the virtualized workload and eliminates the requirement of hardware-based firewalls. One of the characteristics of micro-segmentation is that it is persistent. With micro-segmentation, security policies can be placed on the virtual connections that can move with an application if the network is reconfigured. This makes security on the network persistent as well as ubiquitous. Hence, micro-segmentation enhances the current and future security posture of a network. It is assumed that measure micro-segmentation will be at par with those of conventional segmentation, such as system asset inventory and the items found in BOUND.

C.4.3.4.2 DIGITAL RIGHTS MANAGEMENT (DRM)

Since there are limitations to the tools and methods used to support data-based perimeter protection due to inherent limitation of control mechanisms, DRM provides an alternative method for enforcement of these data-based controls. Enterprise DRM, also commonly referred to as information rights management, provides persistent protection of information regardless of its transience within or external to the enterprise. The DRM tool can be facilitated by a combination of onsite or offsite technology presence (e.g., cloud provided) and should provide sufficient protection mechanisms such that unauthorized access to the data is prevented through strong technical means (e.g., encryption of data) which is capable of being centrally managed by the enterprise. DRM tools should provide some level of assurance that loss of the digital artifacts to an untrusted agent do not necessarily result in the loss of the data contained within. The CDM Program intends to provide supplemental requirements and guidance in forthcoming documentation to clarify the specific mission needs that are necessary under the digital rights management functional area.

C.4.3.4.3 ADVANCED DATA PROTECTIONS

As with DRM, there are limitations to the tools and methods used to support data-based perimeter protection. There are inherent limitations of control mechanisms, advanced data protection safeguards, and the protection of important information from corruption, loss, or exposure to unintended recipients. The term advanced data protection is used to describe both operational considerations such as backup of data and disaster recovery/business continuity, as well as information security considerations such as data classification, access controls, data transformation, and monitoring and auditing. Two functionalities associated with advanced data protection, specifically Data Lifecycle Management (DLM) and Information Lifecycle Management (ILM), are addressed below.

DLM is the automated movement of critical data to online and offline storage and the protections applied to maintain confidentiality, integrity, and availability of that information in the various locations for the specified purpose. Capabilities associated with DLM include, but are not limited to:

a. Encryption and key management.
b. Data masking.
c. Backup and recovery of data.
d. Remote data storage to facilitate disaster recovery.
e. Storage system security.

ILM is the strategy for understanding the value of information and protecting important information assets. Similar to DLM, it operates on the value of data, taking the context of the information into consideration. An example of the difference between DLM and ILM is the information that comprises Personal Identifiable Information (PII) and Sensitive Personal Identifiable Information (SPII). PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. SPII is PII, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements such as Social Security Number (SSN), driver's license number, passport number, biometric identifiers, etc. Other information such as citizenship, medical information, date of birth, or account passwords is sensitive when associated with the identity of an individual. Capabilities associated with ILM include, but are not limited to:

a. Discovery and classification of data.
b. Data vaulting.
c. Data labeling.
d. Data masking and sub-setting.
e. Data access firewall.
f. Data access monitoring.
g. Normalized repository of auditing data.

C.4.4 IT DELIVERY MODELS

The CDM Solution must recognize and incorporate the IT delivery models in place at the Group D Agencies. The following discussion describes models that may be implemented at the Group D Agencies.

Information on whether each Agency uses the centralized or federated model will be noted in the Government-provided, Agency-specific IT/Network Environment Summary Information available in the eRR.

a. Centralized Model. In the centralized model, top-down responsibility for IT acquisition, solutions delivery, conceptualizing, developing, and implementing IT solutions for all parts of the business is controlled by the Agency in one place. This is usually a Headquarters (HQ) function, but may also be delegated to one of the Agency's larger components.

b. Federated Model. In the federated model, the Agency HQ IT unit (usually the Chief Information Officer/Chief Information Security Officer's (CIO/CISO's) office) may have primary responsibility for architecture, common infrastructure and services, and standards decisions, while each Agency IT department has primary responsibility for application resource decisions. Agency IT managers report to the Agency Director as well as the central IT organization. In a few Agencies, the federated model is highly decentralized, with the solutions delivery aligned with the Agency component and IT managers reporting to the Agency component Director. When coordination happens, it is achieved in IT management and executive councils.

C.5 REQUEST FOR SERVICE (RFS)

The Government requires a flexible approach to support the evolving CDM technical capabilities in a rapidly changing cybersecurity environment during the entire life of the TO. To address the evolving needs of the supported Agencies, the Government will execute an RFS process that will further define Agency-specific requirements for initial delivery and/or additional support of a CDM capability or service.

The RFS will state the purpose, supported Agency(ies), primary place of performance, anticipated tasks/subtasks required, technical details of the requirement (including references to the CDM Technical Capabilities Requirements Documents, Volume 1 and Volume 2 (**Section J, Attachments Y.1 and Y.2**) when appropriate), other supporting details related to the requirements (e.g., security requirements, expected execution timelines, Government-Furnished Information (GFI), and tailored System Engineering Lifecycle (SELC) requirements), and expected timeline for return of the RFS Response. Each RFS will apply performance-based outcomes and standards as appropriate to the requirement. High quality products and services delivered in a timely and cost-effective manner will be the primary criteria for the work performed under an RFS.

After receiving an RFS, the contractor shall develop and deliver an RFS Response in accordance with **Section C.6.1.12 (Subtask 1.12)**. The contractor shall only execute actions identified in the RFS Response after the Government provides written approval from either the FEDSIM CO or FEDSIM COR. All cost and schedule measures associated with the execution of a specific RFS shall be clearly identified in the Integrated Master Schedule (IMS), cost reports, and invoices.

The RFS Tracking Table (**Section J, Attachment AI**) identifies RFS actions approved for execution during the TO.

C.6 TASKS

The following are the Tasks for this TO:

Task 1: Provide Project Management

Task 2: CDM Solution and Dashboard Support

Task 3: Integrate New CDM Capabilities

Task 4: Expanded Agency Services

Task 5: Surge Cybersecurity Critical Incident Support

C.6.1 TASK 1 – PROVIDE PROJECT MANAGEMENT

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Project Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and Contracting Officer's Representative (COR) and the DHS Technical Point of Contact (TPOC) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

C.6.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall coordinate with the FEDSIM CO to schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (**Section F, Deliverable 03**). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues and travel/product authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, representatives from DHS, including the DHS TPOC, the FEDSIM CO, the FEDSIM COR, and Government representatives from each Agency supported by this TO.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 02**) for review and approval by the FEDSIM COR and DHS TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Introduction of team members and personnel:
    1. Roles and responsibilities, including staffing plan and project organization.
    2. Overview of the contractor's organizational strategy to support varying locations of work and multiple Agencies.
b. Communication Plan/Lines of communication overview (between both the contractor and Government).
c. Updated Draft Transition-In Plan (**Section F, Deliverable 23**) and discussion.
d. TO Management:
    1. Overview of the TO technical approach, including RFS-DHS-0005.
    2. Overview/outline of the draft Project Management Plan (PMP) (**Section F, Deliverable 17**).
    3. Overview of project tasks, schedule, and establishment of performance metrics.
    4. Identified risks and issues and applicable mitigation plans.

5. Overview of the draft IMS (**Section F, Deliverable 20**) (shows major task, milestones, and deliverables; planned and actual start and completion dates for each).
6. Overview of SELC process.
7. Overview of the TO draft Quality Control Plan (QCP) (**Section F, Deliverable 05**).
8. TO logistics.

e. TO Administration:

1. Review of GFI and Government-Furnished Property (GFP).
2. Deliverable process and procedures.
3. Review of Financial Status Reporting format: including DHS reporting, Agency reporting, invoice review and submission procedures (**Section G.2**), and tracking of funds by Client Tracking Number (CTN) and cost savings.
4. Invoice Requirements.
5. Travel notification, process, and reporting.
6. Request to Initiate Purchase (RIP) submission review and approval process.
7. Security requirements/issues/facility/network access procedures.
8. Sensitivity and protection of information.
9. Reporting requirements, (e.g., Monthly Status Report (MSR)).
10. Proposed reports of technical metrics on operation of the CDM Solution as defined in the PMP, to include percentage of tools deployed to applicable assets relative to adjudicated asset scope with the Agency.
11. Review of RFS process (**Section C.5**).
12. Review of Draft Master Repository (**Section C.6.1.2, Section F, Deliverable 14**).
13. Review of Procurement Report format.
14. Review of Problem Notification Report (PNR) process (**Section J, Attachment Q**).
15. Additional administrative items including press releases.

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Report (**Section F, Deliverable 11**) documenting the Kick-Off Meeting discussion and capturing any action items.

C.6.1.2 SUBTASK 1.2 – MAINTAIN A MASTER REPOSITORY

The contractor shall develop and maintain a Master Repository (**Section F, Deliverables 14, 15, and 16**) of all submitted RFSs, Travel Authorization Requests (TARs), RIPs, and deliverables. At a minimum, this repository shall include dates submitted and approved by the Government, financial information (i.e., estimated costs and costs invoiced) if applicable, pending Government actions, and any other pertinent information associated with the repository items identified above. The master repository is evolutionary and shall be continuously updated as requests/deliverables are submitted/responded to by the Government.

The contractor shall present a master repository format at the Kick-Off Meeting for Government review. The Government will provide written approval of the proposed format via the FEDSIM

COR and this approved format shall be utilized over the life of the TO. The Government may request updates to the format based on CDM PMO repository requirements and Agency needs. Any changes to the format will be requested in writing via the FEDSIM COR. The contractor shall deliver all contents of the repository on a quarterly basis and upon Government request.

C.6.1.3 SUBTASK 1.3 – PROVIDE MONTHLY STATUS REPORT (MSR) AND CONVENE MONTHLY STATUS BRIEFING

The contractor shall develop and provide an MSR (**Section F, Deliverable 08**) via email to the DHS TPOC and the FEDSIM COR. The MSR shall briefly summarize, by task area, the TO management and technical progress to date, as well as provide the current information indicated below. The purpose of this report is to ensure all stakeholders are informed of key elements of the CDM project at the Agency-level, provide opportunities to allow stakeholder input, and coordinate resolution of risks and issues and change management as required. The MSR shall be prepared in accordance with the Monthly Status Report Template (**Section J, Attachment H**).

The contractor shall conduct a Monthly Status Briefing (**Section F, Deliverable 09**) to brief the FEDSIM COR, DHS TPOC, Agency representatives, and other Government stakeholders on the status of the TO and activities. The Government reserves the right to change this requirement to in-person monthly status meetings as required. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of this meeting in a Meeting Report, including attendance, issues discussed, decisions made, and action items assigned (**Section F, Deliverable 11**).

The Monthly Status Briefing shall include, at a minimum:

a. The status of activities during the reported period, by task area.
b. Project schedule.
c. Financial status overview.
d. Procurement status of tools/ODCs.
e. Status of action items, risks, and issues.
f. Progress to date on all items identified in the list above for the MSR.

C.6.1.4 SUBTASK 1.4 – CONDUCT QUARTERLY IN-PROGRESS REVIEW (IPR) MEETINGS

The contractor shall conduct a formal IPR (**Section F, Deliverable 10**) at a location approved by the Government. The IPR shall provide a forum for Government review of progress, planning, and issues related to TO performance. The contractor shall utilize the PMP in its discussion of TO performance. The IPR shall replace the Monthly Status Briefing Meeting for that month. IPRs shall, at a minimum, include:

a. Program status overview.
b. Status of CDM Solution, including Dashboard, at each Agency.
c. Schedule by task.
d. Previous month and quarter activities by task.

e. Planned activities for next month and quarter by task.
f. Financial status, to include quarterly cost savings report on material and equipment purchases.
g. Staffing status by Agency.
h. Status of risks and issues.
i. Actions required by the Government.

The contractor shall prepare the IPR agenda, Meeting Report (**Section F, Deliverable 11**), and presentation material. IPRs shall be conducted no less than quarterly; however, more frequent IPRs may be required. The IPR is historically attended by an average of seven to 15 total stakeholders, to include contractor personnel, FEDSIM COR, DHS TPOC, Agency representatives, and other key Government stakeholders.

The fourth quarter IPR meeting of each TO year shall act as an overview of the entire TO year and act as a closeout for the ending TO year. The fourth quarter IPR shall include the above IPR requirements, financial reporting information for the year, Master Repository and Procurement Report information for the year, and planned actions required by the contractor and Government.

C.6.1.5 SUBTASK 1.5 – PROVIDE FINANCIAL REPORTING

This TO will receive funds through different funding streams from DHS and each of the Agencies and will require distinct financial tracking throughout the life of the TO. The contractor shall provide a Financial Report of cumulative expenditures monthly (**Section F, Deliverable 13**) to the FEDSIM COR and DHS TPOC that tracks these distinct separate funding streams. The Financial Report shall include as a minimum:

a. Identification of the funding source.
b. Monthly expenditures by CDM Phase, CTN, and TO level from the start of the POP.
c. Project monthly expenditures and labor hours by CTN and TO level starting with the current month through the end of the POP.
d. Funded levels by TO and by Agency.
e. Labor hours incurred to date by TO and by Agency.
f. Funds remaining by RFS and CLIN.
g. Diagram reflecting funding and burn rate by month for the TO and at the Agency level.
h. Cumulative invoiced amounts for each CLIN up to the previous month.
i. Actual current and cumulative dollars expensed for small businesses compared to TO subcontracting goals.

The contractor shall present a Financial Report format at the Project Kick-Off Meeting (**Section C.6.1.1**) for Government review. The Government will provide written approval of the proposed format via the FEDSIM CO or FEDSIM COR, and this approved format shall be utilized for the monthly financial reporting requirement. The Government may request updates to the format based on DHS CDM PMO requirements and Agency needs. Any changes to the format will be requested in writing via the FEDSIM CO or FEDSIM COR.

C.6.1.6 SUBTASK 1.6 - PROCUREMENT REPORT

The contractor shall procure the necessary CDM tools and sensors and any ODCs.

The contractor shall develop a Procurement Report (**Section F, Deliverable 52**) in accordance with the Procurement Report Template (**Section J, Attachment J**) for the CDM tools and ODCs that are required to support the CDM Solution or any new CDM capabilities over the POP of the TO. The Procurement Report shall initially capture the planned procurement of any CDM tools and sensors, and later be updated to capture the lifecycle of Delivery and Acceptance for the CDM tools and sensors. The Procurement Report shall be a living document and is anticipated to be updated periodically throughout the TO and, at a minimum, for the following instances:

a. RIP and/or RFS Reference Number, as applicable.
b. Proposed cost from RIP, actual cost of products purchased; CDM tools Special Item Number (SIN) price comparison, if available.
c. Cost savings to the Government (i.e., discounts).
d. Product dates of order, delivery, receipt of goods by Agency customer, and implementation.
e. The date of expiration for products that require renewal.
f. Execution of **Subtask 3.1** – CDM Technical Planning.
g. Identified changes in a planned procurement of CDM tools or ODCs.

The contractor shall work collaboratively with the DHS CDM PMO and Agencies to manage property accountability, to include the transfer of licenses.

C.6.1.7 SUBTASK 1.7 – PREPARE MEETING AND TRAVEL REPORTS

The contractor shall conduct, attend, and participate in various project- and program-related meetings. These meetings may include, but are not limited to, Integrated Project Team (IPT) brainstorming sessions, program management reviews, technical status reviews, document reviews, and contract status reviews.

a. The contractor shall submit Meeting Reports (**Section F, Deliverable 11**) as requested by the FEDSIM COR and/or DHS TPOC to document results of meetings. The Meeting Reports shall include the following information:
    1. Meeting attendees and their contact information; at a minimum, identify organizations represented.
    2. Meeting dates.
    3. Meeting location.
    4. Meeting agenda.
    5. Purpose of meeting.
    6. Summary of events (issues discussed, decisions made, and action items assigned).
b. The contractor shall submit a Trip Report (**Section F, Deliverable 12; Section J, Attachment P**), as requested by the DHS TPOC and/or FEDSIM COR. The need for a trip report will be identified when the TAR is submitted. The Trip Report shall include the following information:
    1. Personnel traveled.
    2. Dates of travel.
    3. Destination(s).

4. Purpose of trip.
5. Summarized cost of the trip.
6. Approval authority.
7. Summary of events, action items, and deliverables.

C.6.1.8 SUBTASK 1.8 – PREPARE A PMP, IMS, AND QCP

Based on the contractor's proposal in response to the solicitation, the contractor shall prepare and deliver a Draft and Final PMP (**Section F, Deliverables 17 and 18**). The PMP shall address work at the first (parent) and second (component, etc.) levels of the Agency, as appropriate.

The PMP shall contain, at a minimum, the following:

a. Management approach:
    1. Communications and stakeholder management (to include the contractor's organizational chart).
    2. Scope management (to include milestones, tasks, and subtasks required in this TO).
    3. Requirements management.
    4. Quality management.
    5. Staffing management (to include the Project Staffing Plan).
    6. Procurement management.
    7. Logistics management.
    8. RFS Management.
    9. Cost Management.
b. Technical approach:
    1. Work Breakdown Structure (WBS) and WBS dictionary. Include associated responsibilities and partnerships between Government organizations. The WBS should plan for control accounts that allow for tasks to be planned, budgeted, forecasted, and cost collected at a level which allows for summary organized by Agency.
    2. Risk management, including identified risks, issues, and planned mitigation.
    3. Testing.
c. Training approach.

Defect metrics are required, including, but not limited to, reflecting where proposed tools negatively impact Agency assets such as extreme performance latency, or where CDM technical requirements are not satisfied due to error conditions.

The PMP is an evolutionary document that shall be updated annually at a minimum (**Section F, Deliverable 19**). The contractor shall work from the latest Government-approved version of the PMP.

The contractor shall prepare and deliver a Draft and Final IMS (**Section F, Deliverables 20 and 21**) and a Draft and Final QCP (**Section F, Deliverables 05 and 06**) to accompany the PMP as separate deliverables.

The IMS is also an evolutionary document that shall be updated with technical inputs and significant changes as required (**Section F, Deliverable 22**). The contractor shall reflect the Government's requirements in planning for all activities in Tasks 2 through 5 and the tailored DHS or Agency-specific SELC process reviews in the IMS. This includes the Government's requirements that the CDM Solution for each Agency shall be operational as soon as the contractor is able to complete installation, configuration, and required security authorization at individual Agencies. The contractor shall work from the latest Government-approved version of the IMS.

The QCP shall include, but is not limited to, the following:

a. Performance monitoring methods.
b. Performance measures.
c. Approach to ensure that cost, performance, and schedule comply with task planning.
d. Methodology for continuous improvement of processes and procedures, including the identification of service metrics that can be tracked in the TO.
e. Government roles.
f. Contractor roles.

Significant changes represent any alteration, modification, or adjustment to the CDM Solution, cost, or schedule that is sufficiently great or important and worthy of attention in the PMP or IMS. As RFS actions are activated, the IMS shall be updated and resubmitted.

The QCP is also an evolutionary document that shall be updated annually at a minimum (**Section F, Deliverable 07**). The contractor shall work from the latest Government-approved version of the QCP.

C.6.1.9 SUBTASK 1.9 – TRANSITION-IN

The Transition-In Plan shall address the Tasks in **Section C.6**, identifying the roles and responsibilities of the contractor and incumbent, information expected from the incumbent, a draft schedule(s), to include the anticipated timeline for appropriate personnel security processing, and milestones to ensure no disruption of service.

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after the Transition-In period. Each Agency is at a different stage in its implementation of the CDM Solution; therefore, the Transition-In Plan shall account for the differences in Agency implementation and IT environment. The contractor shall begin Transition-In activities when the Government has accepted the final Transition-In Plan (**Section F, Deliverable 23**). The Transition-In Plan will take into account the current CDM Solution, which includes Phase 1 and Phase 2 investments. CDM Solution support is currently being provided under TO2D which expires on September 10, 2018. The contractor shall update the proposed Draft Transition-In Plan (**Section F, Deliverable 23**) submitted with its proposal, as appropriate, and provide a Final Transition-In Plan (**Section F, Deliverable 24**) within ten business days after receipt of Government comments.

C.6.1.10 SUBTASK 1.10 - TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The contractor shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Draft Transition-Out Plan (**Section F, Deliverable 25**) NLT 150 calendar days prior to expiration of the base and each option period and the contractor shall provide a Final Transition-Out Plan (**Section F, Deliverable 26**) NLT 120 calendar days prior to expiration of the TO. The Transition-Out Plan shall be organized by Agency. The Government will work with the contractor to finalize the Transition-Out Plan. The contractor shall identify in the Transition-Out Plan how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. Points of Contact (POCs).
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor to contractor coordination to ensure a low risk transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Configuration settings of COTS tools.
i. Asset management, including license expiration dates, where applicable.
j. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless Transition-Out.

The contractor shall update the Transition-Out Plan (**Section F, Deliverable 27**) annually and quarterly during the final option period. The contractor shall implement its Transition-Out Plan in accordance with the Government-approved Transition-Out Plan and NLT 90 calendar days prior to expiration of the TO. All facilities, equipment, and material utilized by the contractor personnel during performance of the TO shall remain accessible to the contractor personnel during the Transition-Out period pursuant to the applicable security in-processing and out-processing guidelines.

C.6.1.11 SUBTASK 1.11 – COORDINATE AND COMPLETE SELC REVIEWS

The contractor shall coordinate and complete each SELC review detailed in the DHS SELC Process Overview (**Section J, Attachment X**) for each Agency's CDM Solution. Depending on the contractor's implementation schedule, these SELC reviews shall be completed concurrently or separately by the Agency. Agency-specific SELC processes may also be required for Agency-sponsored activities and will be stated in the Agency RFS if needed. Deliverables associated with the SELC gate reviews are defined in **Section J, Attachment X**.

C.6.1.12 SUBTASK 1.12 – DEVELOP REQUEST FOR SERVICE (RFS) RESPONSES

The contractor shall develop and deliver an RFS Response (**Section F, Deliverable 28**) for any Government-provided RFS. The RFS process is described in **Section C.5**. The contractor-developed RFS response shall include a brief overview of the requested services, including any relevant technical details pertinent to the proper execution of the support. In addition, the RFS response shall include a Rough Order of Magnitude (ROM) cost estimate that depicts labor categories and hours by task/subtask, a draft RIP for any CDM tools or supporting ancillary products (i.e., hardware/software) as required , and anticipated travel to meet the requirement.

C.6.2 TASK 2 – CDM SOLUTION AND DASHBOARD SUPPORT

The contractor shall provide CDM Solution and CDM Agency Dashboard support entailing necessary testing and security accreditation support to maintain authorization and providing Tier III support to the CDM Solution. This task also entails updating the CDM Agency Dashboard with each new release of the CDM Agency Dashboard, providing Tier II level support to the CDM Agency Dashboard, and establishing and maintaining operational CDM data feeds from the integration layer to the CDM Agency Dashboard and from the CDM Agency Dashboard to the CDM Federal Dashboard. Both the CDM Agency and CDM Federal Dashboards are developed by the CDM Dashboard provider through another CDM TO. This CDM Dashboard provider will provide releases of the CDM Agency Dashboard and Tier III support for the CDM Agency Dashboard to the contractor. The CDM Federal Dashboard is operated and maintained outside of this TO.

C.6.2.1 SUBTASK 2.1 – PROVIDE ENGINEERING SUPPORT TO CDM SOLUTION INTEGRATION LAYER

The continuous operation of an Agency's CDM Solution is predicated on the proper functioning of the integration layer (as depicted in Area B of **Diagram 2**). The contractor shall provide engineering support to each Agency's integration layer. At a minimum, the support of the integration layer shall include the following activities:

a. Conduct activities to achieve interoperability between deployed CDM-approved products with the integration layer.
b. Provide allowance for the timely and accurate ingestion of data through the integration layer in accordance with Agency standards to ensure the CDM Agency Dashboard data is current.
c. Aggregate CDM tools and sensor data in accordance with Agency processes and procedures in order for the data feeds to output the data to the CDM Agency Dashboard.
d. Conduct activities to ensure data from newly deployed CDM tools and new data feeds are ingested and normalized in the integration layer.
e. Synchronize the desired state communications between the CDM Agency Dashboard and the integration layer in accordance with Agency processes and procedures.
f. Continuously conduct vulnerability assessments of the CDM Solution and:
    1. Inform stakeholders, including Agencies and the DHS TPOC, of remediation of default risk critical/high vulnerabilities in writing.

2. Identify Agency-focused implementation plan known vulnerabilities that merit Agency patching or remediation upon tool deployment.
3. Include, at minimum, CVE and CWE-based scan data.

C.6.2.2 SUBTASK 2.2 – CONDUCT TESTING ON CDM SOLUTION

The contractor shall conduct testing on the CDM Solution and new CDM capabilities prior to deployment into operations. Test activities include the development of the test plan, activities, procedures, and results. The CDM Program Test and Evaluation Master Plan (TEMP) (**Section J, Attachment I**) describes the CDM Program planned test and evaluation activities over the Programs' lifecycle and identifies test evaluation criteria. The TEMP is intended to be a living document and, therefore, requires updates to stay current with CDM Program activities and future capabilities. Agency-level TEMPs must remain consistent with the CDM Program TEMP. Approved TEMPs shall be followed throughout the TO performance. The DHS CDM PMO and/or its designated representatives, which may be other contractors, will observe and/or participate in developmental and/or operational tests and evaluations. The Government may conduct additional operational and security-related assessments of the CDM Solution.

The contractor shall conduct testing on CDM solutions by fulfilling the following:

a. Develop a draft and final Agency-Level TEMP (**Section F, Deliverables 29 and 30**) that ensures the delivery of quality CDM capabilities and continued operation of the deployed CDM Solution to the Agencies supported within this TO, update the TEMP to capture changes in the CDM Program TEMP, and test strategy and new capabilities.
b. The TEMP must be inclusive of all testing activities including, at a minimum:
    1. Testing approach:
        i. Critical test parameters.
        ii. Evaluation criteria.
        iii. Developmental test and evaluation method.
        iv. Operational test and evaluation methods for verifying technical and functional requirements.
        v. Automated test tools.
        vi. Resource management.
        vii. A CDM Solution-specific Requirements Traceability Matrix (RTM) that is consistent with the template in the DHS CDM Independent Verification and Validation (IV&V) Strategy documentation and clearly identifies any requirements that are disputed, changed, or considered untestable for CDM PMO adjudication.
    2. Testing methodologies:
        i. Identify the testing tool sets.
        ii. Provide a description of the intended test environment.
    3. Milestone schedules
c. Participate in Test Readiness Reviews (TRRs), which shall be planned at least ten days prior to each test event, and address all items on the TRR checklist (available in the DHS CDM IV&V Strategy documentation).

d. Present the test readiness information to the CDM Test Team for concurrence that all items have been met in order to proceed to the designated Test Milestone/Event. Deliver Test Cases and Test Plans (**Section F, Deliverable 32**) for a particular CDM capability 15 days before a test event. The Test Cases and Test Plans shall include the test and evaluation strategy, test design, test cases, test procedures, and be consistent with the guidance in the DHS CDM IV&V Strategy documentation, including the Sample Test Plan template.
e. Submit a Test Report (**Section F, Deliverable 33**) following each testing event that is consistent with the Test Report Template available in the DHS CDM IV&V Strategy Document (**Section J, Attachment W**).
f. Develop a testing process that ensures all integrated applications are compatible and interoperable with all deployed Agency CDM Solution components prior to installation within the Agency production environment.
g. Conduct test activities for subsequent updates to the CDM Solution, including deployment of new capabilities, and coordinate with the DHS TPOC and respective Agency representatives for system acceptance.
h. Log and track all test results and problems and make readily available to the DHS TPOC and Agency representatives.
i. Report all major issues that arise from test activities or test results that affect the schedule, and provide recommendations on how to proceed, to the DHS TPOC and Agency representative as soon as it becomes apparent the schedule will be affected.
j. Conduct integration testing activities for the Agency-level CDM Dashboard(s) and the respective CDM Solution.
k. Develop and incorporate the CDM Dashboard integration test activities in the Agency-level TEMP Updates (**Section F, Deliverable 31**) and include, at a minimum:
    1. Interface testing.
    2. Integration testing.
    3. Performance testing (including stress and load tests).
    4. Security testing.
    5. Accessibility testing.
    6. Preparation of test plans and procedures.
    7. Test reports.
    8. Acceptance testing.
l. Conduct end-to-end system testing of the CDM Solution including testing in a test environment and Agency-designated environments, which could include development and testing (dev/test), staging, pre-production, and production. End-to-end system testing shall include, at a minimum:
    1. Final acceptance testing of the CDM Solution including CDM Dashboard.
    2. Scalability (network performance).
    3. Conducting integration testing of hardware, software, and network.
    4. Repeatable processes to accommodate changes in either the CDM Solution or the Agency environment.

m. Conduct Post-Implementation Review (PIR) activities to include the following:
    1. Operational testing in the Agency environment.
    2. Evaluating effectiveness of incorporating the CDM Solution into the Agency's CDM governance program.
n. Participate in the bi-weekly Working-level Integration Product Team (WIPT) meetings with the CDM Test Team and present the status of each Agency's testing activities, test artifacts, test results, concerns, issues or questions, and upcoming testing milestones/event timelines.

C.6.2.3 SUBTASK 2.3 – COORDINATE WITH INDEPENDENT VERIFICATION AND VALIDATION (IV&V) PROVIDER

The contractor shall allow DHS CDM PMO and/or its designated representatives (e.g., IV&V Team) to observe and/or participate in all developmental and/or operational tests and evaluations conducted by the contractor (**Section J, Attachment W**).

The Government may conduct additional operational, security, and accessibility related assessments of the CDM Solution. The contractor shall assist with these assessments as directed by the FEDSIM COR and DHS TPOC.

C.6.2.4 SUBTASK 2.4 – PROVIDE SYSTEMS SECURITY AUTHORIZATION CHANGE MANAGEMENT SUPPORT

The contractor shall ensure the existing CDM Solution at the Agencies maintains system security authorization following the most recent revision of NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

In an effort to maintain system security authorization, the contractor shall update the security accreditation package to account for any new CDM capabilities. The Government anticipates activities in this Subtask to only involve updates to a security package, while **Section C.6.4.6** would provide an Agency with a new Security Accreditation Package.

The contractor shall ensure continued integration of the CDM Solution into each Agency's designated Federal Information Standard Management Act (FISMA) inventory system, which in general is categorized as a General Support System (GSS). The security authorization boundary of the CDM Solution shall be treated as a subsystem to the Agency's GSS.

For the purposes of scoping, all CDM Solutions have been categorized for FIPS 199 as High Confidentiality, High Integrity, and Moderate Availability.

The contractor shall provide systems security authorization support by fulfilling the following:

a. Develop documentation to achieve security authorization, in ongoing authorization format, reflecting Agency-specific control implementations.
b. Update applicable System Security Plans (SSPs) and Standard Operating Procedures (SOPs).
c. Develop a Security Model and Documentation (**Section F, Deliverable 34**) that updates the applicable Accreditation/Authorization Package, generally in the form of a security

control catalog. Provide identification that the security model is the overall security approach to include the catalog of controls.

d. Support Security Test and Evaluation/Security Assessment activities by ensuring availability of the technical team personnel for interviews and artifact collections as required.
e. Create new POA&Ms, update existing POA&Ms, and conduct remediation of findings.
f. Continually integrate the CDM Solution into each Agency's designated FISMA inventory system, which in general is categorized as a GSS.
g. Document changes made to the Agency's CDM Solution in a Security Impact Assessment (**Section F, Deliverable 35**).
h. Conduct vulnerability scans and provide results to Agencies in support of the Agency's Risk Management process and determination if a reauthorization is required.

A CDM Solution deployed to a cloud environment may be required to meet FEDRAMP requirements. In order to meet FEDRAMP requirements, the contractor may be required to subcontractor with a Third-Party Assessment Organization (3PAO) to perform the necessary security assessment on the cloud CDM Solution to ensure it is fully compliant with FEDRAMP requirements.

C.6.2.5 SUBTASK 2.5 – PROVIDE TIER III SUPPORT TO THE CDM SOLUTION

The contractor shall provide Tier III support to the CDM Solution. Tier III support shall include advanced engineering support to include coordination and resolution with Solution Original Equipment Manufacturers (OEMs). All calls determined by Tier II to be related to the CDM Agency Dashboard and not resolved through Tier II shall be forwarded to the CDM Dashboard provider for Tier III support. Tier III resolution may require after-hours support depending on the severity of any identified issues.

C.6.2.6 SUBTASK 2.6 – PROVIDE CDM DASHBOARD TECHNICAL SERVICES

The Government provides iterative releases of the previously installed Agency's CDM Dashboard. The Government's CDM Dashboard provider will provide ongoing support of the CDM Agency Dashboard to the contractor for each release of its CDM Agency Dashboard. The Government's CDM Dashboard provider will train the contractor to install, configure, integrate, and support the CDM Agency Dashboard. The CDM Dashboard provider will maintain and improve the functional processes within CDM Agency Dashboard software.

The Government anticipates between two and three CDM Agency Dashboard releases a year. Typically, CDM Agency Dashboard releases incorporate integration of additional data elements from CDM-approved products for CDM Program Phases 1, 2, 3, and beyond. Integration involves mapping CDM tool and sensor data ingested into the integration layer and then mapping the normalized data up to the CDM Agency Dashboard.

For each release of the CDM Agency Dashboard, the Government also anticipates one to three hot fixes that typically incorporate minor changes such as patches for the system components (e.g., RSA Archer platform) and/or bug fixes for summary data feeds to the CDM Federal Dashboard. The Level of Effort (LOE) to support a hot fix is typically less than the integration support associated with a Dashboard release.

In support of CDM Agency Dashboard Technical Services, the contractor shall:

a. Install, configure, and maintain each release of the Government-provided CDM Agency Dashboard for use by the Agencies. CDM Agency Dashboards are inclusive of all sub-Agency Dashboards.
b. Conduct quality assurance and technical testing for each release of the delivered CDM Agency Dashboard with respect to its interoperation with the CDM Solution.
c. Ensure that each release of the CDM Agency Dashboard interfaces with the CDM Federal Dashboard.
d. Implement hot fixes for continued secure operation of the CDM Agency Dashboard.
e. Install, configure, integrate, and transition the CDM Agency Dashboard to production operations.
f. Maintain data input from a single integrated source to the CDM Agency Dashboard.
g. Maintain a CDM data exchange mechanism for the CDM Agency Dashboard and ensure all installed CDM tool and sensor data is sent to the CDM Agency Dashboard.
h. Conduct consistent testing on any changes to the CDM Agency Dashboard.
i. Provide CDM Agency Dashboard testing support and ensure that all installed CDM capabilities report to the CDM Agency Dashboard consistent with Subtask **C.6.2.2**.
j. Ensure new CDM capabilities integrated at each Agency are reported through the CDM Federal Dashboard.

C.6.2.7 SUBTASK 2.7 – PROVIDE AGENCY CDM DASHBOARD TIER II SUPPORT

The contractor shall provide Tier II support to the CDM Agency Dashboard user community including, but not limited to, the following:

a. In-depth troubleshooting.
b. Specialized knowledge of the CDM Solution and CDM Agency Dashboards for remediation.
c. Elevation of all calls determined to be related to the CDM Agency Dashboard and not resolved through Agency CDM Dashboard Tier II support and forwarding of these calls to the CDM Dashboard Provider for Tier III support.

The Agencies will provide the CDM Agency Dashboard Tier I support. CDM Agency Dashboard Tier I support shall include problem resolution using standard methodologies and basic troubleshooting techniques.

C.6.2.8 SUBTASK 2.8 – OPERATE CDM DATA FEEDS

The contractor shall maintain and enhance the CDM data exchange mechanisms, utilizing the Security Content Automation Protocol (SCAP)-compliant Asset Summary Reporting (ASR) Format, as appropriate, between the following:

a. The CDM Solution integration point and CDM Agency Dashboard(s) (Area B and Area C of **Diagram 2**).
b. All CDM Agency Dashboard(s) (within Area C of **Diagram 2**).

c. The CDM Agency Dashboard(s) to the CDM Federal Dashboard - summary level data only (between Area C and Area D of **Diagram 2**).

The contractor shall maintain and enhance data exchange mechanisms that operate between deployed CDM tools and sensors and the CDM Solution's integration layer (between Area A and B of **Diagram 2**).

C.6.3 TASK 3 – INTEGRATE NEW CDM CAPABILITIES

The Government will identify CDM capabilities that require immediate action for implementation of a specific CDM capability or set of capabilities that have not yet been deployed or are requiring updating into an Agency's infrastructure. CDM capabilities are inclusive of filling gaps in an Agency's current CDM environment, expansion of CDM capabilities through new investments, and the technical refresh of previously installed CDM tools and sensors. CDM capabilities are listed below and defined in the CDM Technical Capabilities Requirements Document Volume 1 (**Section J, Attachment Y.1**).

Phase 1: HWAM, SWAM, CM, VUL

Phase 2: TRUST, BEHAVE, CRED, PRIV

Phase 3: BOUND, MNGEVT, OMI, DBS

Phase 4: Micro-Segmentation, DRM, Advanced Data Protection

In response to the RFS, the contractor shall provide a technical plan. After DHS TPOC Review and written FEDSIM CO or FEDSIM COR approval of the technical plan, the contractor shall purchase, install, configure, and customize the CDM capability to ensure proper operation. The contractor shall thoroughly test the CDM capability before transitioning the operation of the capability to an Agency's designated operations team.

C.6.3.1 SUBTASK 3.1 – CDM TECHNICAL PLANNING

In response to the RFS, the contractor shall provide a technical plan defining its approach to implementation of the specific CDM capability or set of capabilities in an Agency's environment. The CDM Technical Planning task shall integrate the contractor's CDM methods and best practices into a sufficiently detailed technical plan, as described in the following subtasks, to ensure successful implementation and operation of the CDM capability at the Agencies supported by this TO. The plan shall address the need for a CDM capability or solution to be secure and hardened, compliant with typical Federal risk tolerance of zero resident default high, critical vulnerabilities, and configured in a manner consistent with depth and scope of the most recent version of NIST 800-53 control baselines.

C.6.3.1.1 SUBTASK 3.1.1 – VALIDATE CDM CAPABILITY

The validation of a CDM capability consists of two parts:

a. The contractor shall:
    1. Conduct analysis to validate its CDM capability implementation approach against each Agency's existing infrastructure to facilitate CDM Program and IT architecture planning.

2. Report all discrepancies between information provided by the Government and the existing environments.
3. Coordinate the analysis with the respective Agencies.

b. The contractor shall develop an Updated Overview of the CDM Capability (**Section F, Deliverable 36**) for inclusion in the Service Design Review (SDR) SELC review, which includes updates as a result of the analysis.

C.6.3.1.2 SUBTASK 3.1.2 – DEVELOP CONCEPT OF OPERATIONS (CONOPS)

The contractor shall develop a CONOPS (**Section F, Deliverable 37**) that describes how the CDM Solution architecture, adjusted for any new CDM capability, shall meet the CDM requirements for the Group D Agencies in their respective environments.

The CONOPS shall include, at a minimum, the following:

a. How the CDM Solution will change as a result of the new CDM capability, specifically identifying how tools associated with the new CDM capability will cover the network and provide data to the integration layer before passing data to the Agency-level CDM Dashboard and the Federal Dashboard. The CONOPS shall contain the specifics for the underlying CDM Solution infrastructure and how the infrastructure must change to support any new CDM capability.
b. Methodology to incorporate data into useful information to support operational, tactical, and strategic decisions for Agencies.
c. Methodology to integrate data from the CDM Solution to support decision systems for the Group D Agencies, including managing technical refresh and upgrades of multiple products.
d. Incorporate CDM-specified security configuration settings, as they become available, to the appropriate toolset.
e. How the enhancement of the CDM Solution through the additional CDM capability will provide desired and actual state and the resulting difference or defect information of each Agency endpoint necessary to assist the Agency in defect remediation.

C.6.3.1.3 SUBTASK 3.1.3 – PREPARE CDM SOLUTION/CAPABILITY IMPLEMENTATION ARCHITECTURE

The contractor shall develop an Implementation Architecture and Back-Out Plan (**Section F, Deliverable 38**) that shall include the following, at a minimum:

a. Overview graphical representation of the overall CDM Solution.
b. Updates to the CDM Solution that clearly denote the additional CDM capabilities.
c. Technical architecture and specifications.
d. Data architecture and specifications.
e. Interface architecture and specifications.
f. Solution functionality.
g. High-level functional requirements.
h. Operational requirements.

i. Plan for reversing implementation, if necessary.

The CDM Solution Implementation Architecture shall elaborate how the existing CDM Solution will be enhanced through the new CDM capability. The Architecture shall show the entire solution (including the ABCD layers in **Diagram 2**) and shall show connectivity between and across ABCD.

The contractor shall update the CDM Solution Implementation Architecture as appropriate to reflect As-Built documentation as part of PIR and deliver the CDM Solution Implementation Architecture - As-Built Update (**Section F, Deliverable 39**).

C.6.3.2 SUBTASK 3.2 – INSTALL, CONFIGURE, AND CUSTOMIZE CDM CAPABILITY

Based on the requirements of each Agency, the contractor shall install, configure, and/or customize the tools, sensors, and any supporting ancillary products to meet a CDM capability consistent with the Agency's IT/Network Environment Summary Information, additional information disclosed in **Section C.6.3.1**, and with the IMS and PMP. The contractor shall provide the most current version(s) and release(s) of any and all source, object, executable, and run-time code (as applicable) developed under the efforts of this TO ("New Code") and unique enhancements, customization, and plug-ins, and other similar artifacts ("Customizations") to the Government (**Section F, Deliverable 40**) in accordance with the delivery requirements in **Section F.3**.

The contractor shall design its approach to a CDM capability to ensure that the operating CDM Solution has minimal network performance impact as a result of integrating the CDM capability into the CDM Solution. CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**) define minimal impact as, "Limit the burden put on network resources such that the presence of the scan is not noticeable above background variation in network bandwidth."

It is permissible to include free open-source software, free proprietary software, free or priced Government Off-the-Shelf (GOTS) software, or other non-COTS software in the technical plan for implementing new CDM capabilities within an Agency's CDM Solution; however, such software is subject to the Government's approval.

The Government anticipates that no new software development (as opposed to configuration of COTS tools) will be required under this TO. However, in the event that new software development is required, **Section H.17** applies.

C.6.3.3 SUBTASK 3.3 – TRANSITION TO OPERATIONS

After the tools supporting the new CDM capabilities are operational and the solution security authorization has been completed, the contractor shall transition the operation of the solution to the Agency's operations team. The contractor shall provide Agency-designated system administrators full and complete access to the CDM tools and sensors, including their product consoles. The contractor shall be responsible for complete and seamless transition of the overall and Agency-specific solution to each Agency's operations team.

The contractor shall develop a Plan for Transition to Agency Production Operations (**Section F, Deliverable 41**) describing how the contractor shall transition production operations of the

modified CDM Solution to the Agency's operations team. The plan for transition to Agency production operations shall include the following elements:

a. Testing Methodology (in support of **Section C.6.2.2**) to include the TEMP.
b. Implementation Methodology, to include the contractor's plan to:
    1. Provide considerations for risk mitigation such as the following:
        i. Demonstration of CDM capability and CDM Solution implementation in lab environment.
        ii. Initial pilot to test the CDM infrastructure with defined success criteria.
        iii. Phased implementation approach.
        iv. User acceptance testing.
        v. Submission of software as part of baseline configuration image.
    2. Roll-out of functionality consistent with IMS.
    3. Documentation of Agency Dependencies (**Section F, Deliverable 42**).
    4. Description of configuration management methodology for the tools and sensors of the Agency's CDM Solution.
c. Transition to Agency Operations Team:
    1. Provide training and support to Agency-designated/existing staff to ensure a smooth transition. The training shall be inclusive of the implementation and operation of the specific CDM capability in the Agency's CDM Solution, including the operation of any CDM tools that are implemented to support the CDM capability.
    2. Collect operational requirements needed within the Agencies to operate the solution through the entire life of the TO.
    3. Confirm with Agency Operations Team under the governance of the DHS CDM PMO and the Agencies:
        i. Detailed activities that support the CONOPS.
        ii. Configuration control.
        iii. Change control management.

The Agency's Production Operations will operate the solution in production after installation and integration in accordance with the Plan for Transition to Agency Production Operations and the IMS.

The contractor shall work in conjunction with the Agency's Production Operations, as well as the FEDSIM COR, DHS TPOC, and the respective Agency, to perform the following:

a. Provide training to the Agency's Production Operations. Provide training and support to Agency-designated/existing staff to ensure a smooth transition.
b. Monitor the solution for system performance and functionality.
c. Incorporate the solution into the respective Agency's continuous monitoring activities.
d. Ensure the solution operates consistent with the Agency system security requirements.
e. Perform problem management in coordination with the Agencies for the solution by identifying problems and performing resolution, to include notifying vendors of

application issues. The contractor is expected to continue to provide Tier III (engineering level) support through the POP of the TO in accordance with **C.6.2.5**.

f. Initiate formal requests for any Agency infrastructure modifications and follow change control procedures.

C.6.4 TASK 4 – EXPANDED AGENCY SERVICES (Optional)

Group D Agencies may elect to receive services defined in the following subtasks. The Government anticipates utilizing the RFS process to initiate contractual actions which will execute the subtasks described in detail below.

C.6.4.1 SUBTASK 4.1 – OPERATE AND MAINTAIN CDM SOLUTION

The contractor shall conduct the O&M of the CDM Solution, including the installed suite of CDM tools and sensors. This support may be provided either on-site at the Agency's location(s), from the contractor's facility, from an alternate location, or in combination. While Agency-designated system administrators will have access to the CDM tools and sensors, including their product consoles, the contractor shall be responsible for the operation of the overall CDM Solution. The operational requirements in this task apply to the CDM Solution, to include the Agency CDM Dashboard and associated data feeds, as identified in Areas A, B, and C of **Diagram 2: CDM Architecture** (**Section C.4.1**).

C.6.4.1.1 SUBTASK 4.1.1 – PROVIDE TIER II SUPPORT TO THE CDM SOLUTION

The contractor shall provide Tier II services for the Agency's CDM solution, coordinating with the Agency's and CDM Dashboard Provider's Help Desks. The contractor shall provide hotline capability during the normal workweek (Monday through Friday) and shall provide coverage from 8:00 a.m. through 6:00 p.m. Eastern Time (ET). In some instances, 24 hours a day and seven days a week support may be necessary and will be identified in an RFS.

a. The Agencies will provide all Tier I support. Tier I support will include problem resolution using standard methodologies and basic troubleshooting techniques including Agency-raised issues, incident and request management, access and inventory management, change and configuration management, security, and patch management consistent with the Agency's policies and procedures.
b. The contractor shall provide Tier II support for the Agency CDM Solution. Tier II support shall include more in-depth troubleshooting and shall require specialized knowledge of the CDM Solution for remediation.
c. Tier III support to CDM Solution is provided under **C.6.2.5.**

The contractor shall establish a procedure for recording and a ticket tracking mechanism for all operational support requests. On a monthly basis in the MSR (**Section C.6.1.3**), the contractor shall report the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved. The contractor shall, at a minimum, provide the following support:

a. Provide initial problem resolution where possible.
b. Generate, monitor, and track incidents through resolution.
c. Provide software support.

d. Maintain Frequently Asked Questions (FAQs) (**Section F, Deliverable 43**) and their resolutions.
e. Obtain customer feedback and conduct surveys.

C.6.4.1.2 SUBTASK 4.1.2 – PREPARE AND EXECUTE A PLAN FOR PRODUCTION OPERATIONS

The contractor shall develop a Plan for Production Operations (**Section F, Deliverable 44**). The Plan for Production Operations shall describe how the contractor intends to operate the CDM Solution. The Plan for Production Operations shall describe the O&M methodology to supporting the CDM Solution at a particular Agency and shall, at a minimum:

a. Identify requirements needed to operate the CDM Solution through the entire life of the TO.
b. Provide a description of detailed activities that support the CONOPS.
c. Determine data relevant for inclusion in the MSR.
d. Provide a description of the Operational Analysis (**Section F, Deliverable 45**) for PIRs.
e. Describe the configuration management methodology for the tools and sensors of the CDM Solution.
f. Incorporate CDM services on all assets of the Agency's infrastructure, including applications, servers, and desktops.
g. Describe the Change Management methodology for the tools and sensors of the CDM Solution.
h. Incorporate and support Agency-specific Service Level Agreements (SLAs).

The contractor shall operate the CDM Solution consistent with the approved Plan for Production Operations. The contractor shall monitor the CDM Solution for system performance and functionality and elevate any issues. The contractor shall incorporate the CDM Solution into the respective Agency's continuous monitoring activities. The CDM Solution shall operate consistent with the system security requirements. The contractor shall proactively monitor CDM tools for potential disruptions to Agency systems and other security capabilities.

The contractor shall perform problem management in coordination with the Agencies for the CDM Solution by identifying problems and performing resolution, to include notifying OEM vendors of application issues. The contractor shall initiate formal requests for any Agency infrastructure modifications and follow change control procedures. The contractor shall provide technical support for all CDM Solution components and the solution as a whole, whether from a single source or multiple sources.

C.6.4.1.3 SUBTASK 4.1.3 – PERFORM SYSTEM ADMINISTRATION

The contractor shall perform system administration to operate the CDM Solution throughout the TO POP. The contractor shall, at a minimum, provide the following support pending Agency change management approval:

a. Patching.
b. Upgrades.
c. Replacement of failed components of the CDM Solution.

C.6.4.2 SUBTASK 4.2 – PROVIDE GOVERNANCE SUPPORT

Governance is a necessary component for ensuring effective integration of technology into an Agency's cybersecurity program. Agencies are responsible for managing and maintaining cybersecurity-specific controls by linking technologies with effective policies and procedures in order to comply with Office of Management and Budget (OMB) guidelines, often described as an Agency's Information Security Continuous Monitoring (ISCM) program.

The contractor shall assist Agencies in incorporating CDM capabilities into each Agency's specific cybersecurity or ISCM program so that the following outcomes are effectively planned, implemented, and documented:

a. Increased and/or more efficient risk reduction (also described as defect reduction) at Agencies utilizing the most current CDM Agency Dashboard release and supporting technologies.
b. Improved definitions of, or criteria related to, Agency risk thresholds relative to the CDM architecture and any extant Agency policies or plans related to ISCM.
c. Identification or improved definition of Agency-specific "desired states" for use within the CDM architecture in general and current CDM Agency Dashboards and supporting tools in particular, so defect reduction is more effectively or efficiently realized, and Agency machine-level policies for future automated ongoing assessment of current, applicable NIST SP 800-53 controls are met.

C.6.4.2.1 SUBTASK 4.2.1 – ASSESS AND SUPPORT AGENCY CDM GOVERNANCE

The contractor shall deliver a draft and final As-Is Governance Report (**Section F, Deliverable 46**) for each supported Agency. The As-Is Governance Report shall include an analysis of the current ability of an Agency to leverage CDM information to reduce risk and mitigate defects. The As-Is Governance Report shall also include at a minimum the following:

a. Analysis of any existing Agency-specific Governance Support Plan, as developed during CDM Phase 1 and Phase 2 orders, and how successful the implementation of that Plan has been to support CDM policies.
b. A review of existing ISCM governance structures (charters, policies, memos, procedures, organization structures, and relationships) and how each is utilized in the use of CDM-supplied data for risk management activities.
c. A review of Agency workforce planning efforts in the identification and establishment of an information security workforce that supports the use of CDM-supplied data for risk management activities.
d. A review of Agency efforts in planning for the continued support of CDM capabilities and maintenance of an ISCM program.

The contractor shall deliver a draft and final CDM Governance Enhancement Plan (**Section F, Deliverables 47 and 48**) for the Group D Agencies. The CDM Governance Enhancement Plan shall provide the Agency with tailored recommendations and best practices to further enhance the Agency's cybersecurity governance posture; improve Agency-specific CDM governance structures and policies; and establish, modify, improve, and manage each Agency's ISCM Program, with a focus towards risk reduction and defect mitigation. At a minimum, the CDM Governance Enhancement Plan shall include the following:

a. A process to develop or improve and manage Agency-specific ISCM governance structure based on gaps identified in the Governance Assessment Report. This includes identifying any additional policies, procedures, SOPs, and other security documentation that may be required.
b. An approach to integrate CDM capabilities and Federal- and Agency-level Dashboard metrics into Agency ISCM or broader cybersecurity governance structures and policies.
c. A strategy to develop, align, or update an Agency's ISCM strategy and approach with Federal requirements including, but not limited to, the following:
    1. OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*.
    2. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*.
    3. NIST SP 800-37 rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*.
    4. 2016 IG FISMA Metrics, Section 3.0.
    5. Current Cross Agency Priority (CAP) Goals for Cybersecurity.
d. Tailored recommendations to employ CDM tools beyond CDM requirements to better enable or automate defect reduction, such as:
    1. Tailored best practice guidelines on utilizing applicable CDM tools to perform network access control to minimize HWAM defects from negatively impacting Agency risk thresholds and metrics.
    2. Further automation of previously manual cybersecurity controls or capabilities through use of the CDM tools and architecture and suggestions of how better to utilize cyber staff as a result.
    3. Furthering support of Application Whitelisting (AWL) via applicable CDM tools, tailored to Agency process and structure and degree of federation, so that defect-reducing outcomes described above are supported.
    4. Orchestration with existing service desk ticketing and/or network monitoring systems.
    5. Use of authoritative HWAM asset data for streamlined FISMA boundary delta updates to incorporate relevant stakeholders.
    6. Expansion of CDM tool functionality to consider inclusion of development networks and development oversight.
e. Identification of any additional support to further expand governance support required to support each Agency's CISO.

The contractor shall host bi-weekly Inter-Agency governance coordination meetings. The contractor shall maintain invitations and continuously solicit participation for the appropriate stakeholders based on meeting topics. The contractor shall lead the meeting and maintain the meeting agenda, a repository of meeting summaries, and a repository of lessons learned (**Section F.3, Deliverable 11**).

In addition, the contractor shall host CDM working groups at each individual Agency as needed to focus on prioritizing and addressing any suggested governance updates.

C.6.4.2.2 SUBTASK 4.2.2 – DEVELOP AND UPDATE ISCM GOVERNANCE DOCTRINE

Agencies will execute additional governance support as needed to fill identified gaps in existing security doctrine.

Based on the approved CDM Governance Support, the contractor shall develop and deliver CDM Governance Documentation (**Section F, Deliverable 49**) that shall assist Agencies with strengthening security programs through additional controls. CDM Governance Documentation shall consist of, but is not limited to, the following:

a. SOPs.
b. Policy.
c. Procedures.
d. Directives.

The contractor shall deliver a CDM Communications Plan (**Section F, Deliverable 50**), which shall assist Agencies with managing internal communication efforts related to CDM. At a minimum, the CDM Communications Plan shall include the following:

a. A strategy to increase effectiveness of internal CDM activities.
b. A communications approach for varying audiences depending on CDM impacts.
c. A roadmap for continued communication.

C.6.4.3 SUBTASK 4.3 – PROVIDE CDM SOLUTION TRAINING

The contractor shall provide training on implementation and operation of an Agency's CDM Solution, including the operation of individual CDM tools.

The contractor shall deliver CDM Solution Training Plan Documentation (**Section F, Deliverable 51**) consisting of all training materials, any training manuals, COTS manuals for all installed CDM-related tools, and a Training Plan for each Group D Agency. At a minimum, the Training Plan shall include the following:

a. Training method.
b. Training medium.
c. Training tools.
d. Frequency of training.
e. Audience.
f. Location.
g. Method to incorporate training feedback.

The contractor shall ensure all training is consistent with the DHS-provided CDM Program training content. The DHS CDM training content provides an overview of CDM concepts, principles, and approaches for all phases of the CDM Program and how CDM capabilities work together.

At a minimum, the contractor shall deliver the following CDM Solution-based training:

a. **CDM Solution Overview Training**. The contractor shall conduct this training prior to deploying new CDM capabilities in an Agency's CDM environment. This training shall include detailed information on how the Agency can operationalize CDM Dashboard metrics.
b. **CDM Solution Technical Training**. The contractor shall provide training on the CDM Solution product configuration, integration, and operations as they relate to an Agency's network environment. This training is not intended to replace manufacturer's certification training. This training shall be role-based and consist of two subsets of training; specifically:
    1. CDM Tools-specific hands-on training for the user community, which allows the end-user to experience operations and the use of specific tools at the Agency, including vendor-based product training. This training can be provided at a contractor facility, virtually, or at the Agency site.
    2. Scenario-based training that exposes users to real-world use of the entire CDM Solution. This training can be provided at a contractor facility, virtually, or at the Agency site.
c. **CDM Agency Dashboard Technical Training**. This training shall include hands-on training on how certain users can operate the delivered Agency Dashboard.

The CDM Agency and Federal Dashboard provider will provide standardized FOC CDM Dashboard training materials to the contractor when delivering the CDM Agency Dashboard training. The contractor shall present content specific to the CDM Solution as it relates to the standardized CDM Agency Dashboard training content with consideration of Agency unique environments.

C.6.4.4 SUBTASK 4.4 – PROVIDE CDM ASSET MANAGEMENT TRACKING

The contractor shall track IT assets leveraging IT asset information gained through the CDM Phase 1 implementation and shall assist the Agency with efforts to centralize IT license management. The contractor shall recommend strategies and practices that reduce duplicative IT purchases and streamline the purchase of maintenance on existing IT investments. The contractor shall institute processes that alert Agency representatives of funding requirements for the continuing maintenance of the IT investments.

In addition, the contractor shall provide an Agency-Specific Software License Inventory (**Section F, Deliverable 53**), including all licenses purchased, deployed, and in use, as well as spending on subscription services, to include provisional (i.e., cloud) Software as a Service (SaaS) agreements. The contractor shall analyze inventory data to ensure compliance with software license agreements, consolidate redundant applications, and identify other cost-saving opportunities.

C.6.4.5 SUBTASK 4.5 – INTEGRATE AGENCY DATA AND APPLICATION INTO THE CDM SOLUTION

Agencies may have applications that require integration into the CDM Solution for the purposes of data sharing. The contractor shall integrate and maintain interoperability between the CDM Solution and other Agency legacy applications for the purpose of sharing data.

The contractor shall establish the data exchange mechanism between the CDM Solution and Agency applications that hold the necessary information. Examples of applications include, but are not limited to, the following:

a. Discovery tools.
b. Network asset systems (e.g., Active Directory and other Lightweight Directory Access Protocol (LDAP)-like systems).
c. Property management systems.
d. Configuration management systems.
e. Vulnerability management systems.
f. Open Checklist Interactive Language (OCIL) questionnaire systems.

The contractor shall periodically perform the appropriate data exchanges between the Agency legacy applications and the CDM Solution to ensure the CDM Solution uses the most current data as defined by the Agency policy. The contractor shall update the data exchange mechanism in response to changes in either the Agency applications or the CDM Solution.

C.6.4.6 SUBTASK 4.6 – PROVIDE SYSTEMS SECURITY AUTHORIZATION SUPPORT

The contractor shall provide System Security Authorization support to develop new or replacement security accreditation packages for the deployed CDM Solution.

In accordance with the FISMA, the CDM Solution at each Agency is required to receive/maintain system security authorization following the most recent version of NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The contractor shall support the Agency's System Accreditation and ongoing authorization processes and activities to ensure that the implementation of the security controls maintain effectiveness over time. These activities include, but are not limited to, the following:

a. Provide the Agencies with new or replacement documentation to support the Agencies' security authorization (in ongoing authorization format). This includes control implementation updates in applicable SSPs and SOP updates as applicable.
b. Provide technical support to the Agency's security authorization process related to the CDM Solution:
    1. Support Security Test and Evaluation/Security Assessment activities by ensuring availability of the technical team personnel for interviews and artifact collections as required.
    2. POA&M Management:
        i. Remediation and updates to existing POA&Ms.
        ii. Creation of new POA&Ms.

Any portion of an Agency's CDM solution that is deployed and resides in a cloud environment may be required to meet FEDRAMP requirements. In order to meet FEDRAMP requirements, the contractor may be required to subcontract with a 3PAO to perform the necessary security

assessment on a specific CDM cloud solution to ensure it is fully compliant with FEDRAMP requirements.

C.6.4.7 SUBTASK 4.7 – PROVIDE CONTINUOUS AGENCY ISCM STRATEGIC AND CIO/CISO PROGRAMMATIC SUPPORT

Each Agency will consider longer term strategic objectives of their ISCM programs and how CDM can be leveraged to support the achievement of those objectives. Agencies will require additional programmatic support to assist in the establishment and transformation of CISO and CIO program offices to support the strategic direction of the Agency's ISCM program.

The contractor shall provide support for this process that consists of:

a. Establishing and transforming CIO and CISO program offices that leverage CDM capabilities to meet strategic objective and inform data-driven decision making to reduce Agency cyber risk.
b. Developing policies, processes, and procedures that support the operationalization of:
    1. Security objectives outlined in the Agency's ISCM Strategy.
    2. Federal policies, regulations, guidelines, and standards.
c. Developing, implementing, and operating a configuration management approach that aligns with the capabilities provided by the CDM Solution.
d. Development, implementation, and operation of a knowledge management approach.

C.6.5 TASK 5 – SURGE CYBERSECURITY CRITICAL INCIDENT SUPPORT (Optional)

The Government anticipates surge support will be required on a case-by-case basis when Agencies supported by this TO are impacted by cyber-attacks, in need of penetration testing, or require cyber risk assessment and mitigation activities. The scope of the response shall consist of conducting an initial assessment of the attack, identifying a plan of action, and implementing the approved response.

The Government plans to initiate surge support services using the RFS process (**Section C.5**). The Government will provide the requirements for the timing of the contractor's response upon initiating the support. Surge support shall not result in a decrease of support to other TO requirements unless approved by the FEDSIM CO and FEDSIM COR.

The following applies to performing the cyber-attack surge support:

a. The Government will estimate the scope of surge support required at the time of the cyber-attack.
b. The contractor may be required to provide surge support at Agency spaces.
c. Once a cyber-attack response has ended, the contractor shall proceed with an orderly and efficient transition-out period. During the transition-out period, the contractor shall fully cooperate with, and assist the Government with, activities closing out the matter, developing required documentation, transferring knowledge, training, and lessons learned.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the FEDSIM COR. Inspection will occur at FEDSIM, DHS, and Agency locations.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and DHS TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be in compliance with the requirements set forth in the TO, , and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government’s comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government’s satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in **Section F**) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government’s comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO/COR will provide written notification of acceptance or rejection (**Section J, Attachment T**) of all final deliverables within 15 workdays (unless specified otherwise in **Section F**). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated impact to the award fee earned.

E.7 HARDWARE AND SOFTWARE PRODUCT DELIVERY

The contractor shall fill out the Requisition and Invoice/Shipping Document (DD1149) (**Section J, Attachment M**) on an as-needed basis. The DD1149 shall act as Agency acknowledgment that a hardware or software product will be shipped. The Material Inspection and Receiving Report (DD250), (**Section J, Attachment N**) will serve as formal acceptance of the products after delivery and is always required. The DD1149 (when required) and DD250 shall be signed by appropriate Agency representatives that will be identified after TOA.

The hardware/software products shall be delivered to the Agencies in the Continental United States (CONUS) and occasionally Outside of the Continental United States (OCONUS). The contractor shall deliver these products in accordance with the IMS. A copy of each document shall also be sent to the FEDSIM COR and DHS TPOC.

Specific places of delivery for hardware/software products will be provided after TOA.

F.1 PERIOD OF PERFORMANCE (POP)

The POP for this TO is as follows:

Base Period:	August 06, 2018 through August 05, 2019
First Option Period:	August 06, 2019 through Febuary 29, 2020

The remaining POP below, including the second half of First Option Period, will continue under PIID 47QFRA20F0016.

First Option Period:	March 01, 2020 through August 05, 2020
Second Option Period:	August 06, 2020 through August 05, 2021
Third Option Period:	August 06, 2021 through August 05, 2022
Fourth Option Period:	August 06, 2022 through August 05, 2023
Fifth Option Period:	August 06, 2023 through April 30, 2024

F.2 PLACE OF PERFORMANCE

The place of performance for the TO is primarily the contractor's facility. Work will also be performed at Agencies located within the Washington, District of Columbia (D.C.), National Capital Region (NCR). The contractor's facility shall include spaces suitable for a development and test facility and to support classified IT storage. The contractor shall have access to a facility with a Top Secret (TS) accreditation level.

Implementation activities may require travel to and work to be performed at various Agency locations, both offices and data centers, across the CONUS and possibly OCONUS locations.

F.3 TASK ORDER SCHEDULE OF DELIVERABLES AND MILESTONE DATES

The following schedule of deliverables and milestones will be used by the FEDSIM COR to monitor timely progress under this TO. The following abbreviations are used in this schedule:

DEL: Deliverable
IAW: In Accordance With
NLT: No Later Than
TOA: Task Order Award
All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Abbreviations in the Data Rights Clause (Gov't Rights**) column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14
RS: Restricted Software, per FAR 27.404-2 and 52.227-14
LD: Limited Rights Data, per FAR 27.404-2 and 52.227-14

SW: Special Works, per FAR 27.405-1 and 52.227-17

For software or documents that may be either proprietary COTS or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The data rights in open source COTS software will be as set forth in open source license agreements accompanying them, provided that in case of conflict, the GSAM Clauses stated in section I.2 will govern and be deemed to amend such license agreements to the extent of the conflict. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TOR **Section H.14**. For purposes of the foregoing, the terms "collateral agreement," "Supplier Agreement," and "Commercial Supplier Agreement" have the same meaning.

The contractor shall deliver the deliverables listed in the following table on the dates specified. All deliverables shall be named using the naming convention of "DEFEND_GrpD_Del#_Deliverable Name_mm-yy" (e.g., DEFEND_GrpD_05_QCP-Draft_Jan-18).

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS**
01	Project Start (PS)	N/A	August 06, 2018	N/A
02	Kick-Off Meeting Agenda & Presentation	C.6.1.1	At least 3 workdays prior to the Kick-Off Meeting	UR
03	Kick-Off Meeting	C.6.1.1	Within 20 workdays of TOA	N/A
04	Redacted copy of Task Order (TO) (initial award and all modifications)	F.4	Within 10 workdays of award	N/A
05	Quality Control Plan -- Draft	C.6.1.1 C.6.1.8	Submitted at Kick-Off Meeting	UR
06	Quality Control Plan – Final	C.6.1.8	10 workdays after receipt of Government comments	UR
07	Quality Control Plan Updates	C.6.1.8	As changes in program processes are identified	UR
08	Monthly Status Report (MSR)	C.6.1.3	Monthly, 10th calendar day of the next month	UR
09	Monthly Contract Activity and Status Briefing	C.6.1.3	Monthly, 15th calendar day of the next month	N/A
10	In-Progress Review (IPR)	C.6.1.4	Quarterly	UR
11	Meeting Reports	C.6.1.1 C.6.1.3 C.6.1.4 C.6.1.7 C.6.4.2.1	Within 5 workdays of the meetings	UR
12	Trip Report(s)	C.6.1.7	Within 5 workdays following completion of each trip	UR

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS**
13	Financial Report	C.6.1.5	Monthly, 10th calendar day of the next month	N/A
14	Master Repository - Draft	C.6.1.1 C.6.1.2	Due at Kick-Off Meeting	UR
15	Master Repository - Final	C.6.1.2	10 workdays after receipt of Government comments	UR
16	Master Repository - Updates	C.6.1.2	Quarterly or upon Government request	UR
17	Project Management Plan (PMP) - Draft	C.6.1.1 C.6.1.8	Due at Kick-Off Meeting	UR
18	PMP - Final	C.6.1.8	10 workdays after receipt of Government comments	UR
19	PMP - Updates	C.6.1.8	As project changes occur, no less frequently than annually	UR
20	Integrated Master Schedule (IMS) – Draft	C.6.1.1 C.6.1.8	Due at Kick-Off Meeting	UR
21	IMS – Final	C.6.1.8	10 workdays after receipt of Government comments	UR
22	IMS – Updates	C.6.1.8	As project changes occur, no less frequently than annually	UR
23	Transition-In Plan – Draft	C.6.1.1 C.6.1.9	Submitted with Proposal; Reviewed at Kick-Off Meeting	UR
24	Transition-In Plan – Final	C.6.1.9	10 workdays after receipt of Government comments	UR
25	Transition-Out Plan – Draft	C.6.1.10	NLT 150 calendar days prior to expiration of the base period	UR
26	Transition-Out Plan – Final	C.6.1.10	NLT 120 days prior to expiration of TO	UR
27	Transition-Out Plan Updates	C.6.1.10	Annually and then quarterly during final Option Period	UR
28	Request for Service (RFS) Response	C.6.1.12	NLT 15 workdays after receipt of RFS unless otherwise specified	UR
29	Test and Evaluation Master Plan (TEMP) - Draft	C.6.2.2	Within 5 workdays of Kick-Off Meeting	UR
30	TEMP – Final	C.6.2.2	10 workdays after receipt of Government comments	UR

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS**
31	TEMP – Updates	C.6.2.2	As project changes occur, annually at minimum	UR
32	Test Cases and Test Plans	C.6.2.2	15 workdays prior to a test event	UR
33	Test Report	C.6.2.2	Within 5 workdays of a test event	UR
34	Security Model and Documentation	C.6.2.4	IAW IMS	UR
35	Security Impact Assessment	C.6.2.4	IAW IMS	UR
36	Updated Overview of the CDM Capability	C.6.3.1.1	IAW IMS	UR
37	Concept of Operations (CONOPS)	C.6.3.1.2	IAW IMS	UR
38	Implementation Architecture and Back-Out Plan	C.6.3.1.3	IAW IMS	UR
39	CDM Solution Implementation Architecture – As-Built Update	C.6.3.1.3	IAW IMS	UR
40	New Software – Source, Object, Executable, and Run-Time Code	C.6.3.2 F.3.1	IAW IMS	UR
41	Plan for Transition to Agency Production Operations	C.6.3.3	IAW IMS	UR
42	Documentation of Agency Dependencies	C.6.3.3	IAW IMS	UR
43	Frequently Asked Questions (FAQs)	C.6.4.1.1	IAW IMS	UR
44	Plan for Production Operations	C.6.4.1.2	IAW IMS	UR
45	Operational Analysis	C.6.4.1.2	IAW IMS	UR
46	As-Is Governance Report	C.6.4.2.1	IAW IMS	UR
47	CDM Governance Enhancement Plan – Draft	C.6.4.2.1	IAW IMS	UR
48	CDM Governance Enhance Plan – Final	C.6.4.2.1	IAW IMS	UR
49	CDM Governance Documentation	C.6.4.2.2	IAW IMS	UR
50	CDM Communications Plan	C.6.4.2.2	IAW IMS	UR

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS**
51	CDM Solution Training Plan Documentation	C.6.4.3	IAW IMS	UR
52	Procurement Report	C.6.1.6	Monthly, 10th calendar day of each month	N/A
53	Agency-Specific Software License Inventory	C.6.4.4	IAW IMS	N/A
54	Supply Chain Risk Management (SCRM) Plan	H.6.4.1	As needed	N/A

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.3.1 SOURCE, OBJECT, EXECUTABLE, AND RUN-TIME CODE

The contractor shall provide the most current version(s) and release(s) of any and all source, object, executable, and run-time code ("New Code") (as applicable) developed under the efforts of this TO and unique enhancements, customization, and plug-ins, and other similar artifacts ("Customizations") to the Government (**Section F, Deliverable 40**) in accordance with the delivery requirements in **Section F.3**. The parties agree that payments made under this TO constitute full payment for any data rights in New Code. The Government's requirements for data rights in the New Code and Customizations are specified in **Section F.3**, and FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007). The contractor shall ensure that all COTS licenses and open source licenses both allow for the creation of the customizations and vest the data rights to the customizations exclusively in the Government.

DHS CDM PMO will have unlimited rights to use and modify all source, object, executable, and run-time code (as applicable) comprising the New Code and its associated documentation, even in the event that the contractor shall become unable to continue supporting the CDM Solution. The contractor, immediately upon delivery (each deliverable accompanied by a signed assignment of copyright), shall assign copyright in such New Code to the Government as contemplated under the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007). Source, object, executable, and run-time code (as applicable), including scripts and enhancements, comprising the New Code for releases of the software produced under this TO shall become the property of the Government upon such assignment. The source, object, executable, and run-time code (as applicable), with its associated documentation and other materials as specified in **Section F.3**, shall be delivered to the DHS CDM PMO on dates established in accordance with **Section F.3**, but in any event, NLT 30 calendar days following the termination/expiration of the TO. In the event the contractor defaults on the terms of this TO for any reason, the most current version of the source, object, executable, and run-time code shall be delivered to DHS CDM PMO NLT 30 calendar days following the event that leads to the termination/expiration of the TO. The Government will retain the right to use any and all

versions that are at that time installed at a Government facility and to further develop and distribute them, with no further royalties or other payments being due to the contractor or any other party.

The contractor may request and the Government may grant different or more restrictive rights, such as special works rights, than are depicted in the preceding table, in which event the table will be updated and incorporated into the TO. The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document (**Section F, Deliverable 04**) with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 United States Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in the Master Repository (**Section C.6.1.2**). The following are the required Microsoft (MS) electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text MS Word
b. Spreadsheets MS Excel
c. Briefings MS PowerPoint
d. Drawings MS Visio
e. Schedules MS Project

F.6 PLACE(S) OF DELIVERY

All deliverables shall be delivered to the FEDSIM COR at the following address:

To be provided at award.

Copies of all deliverables shall also be delivered to the DHS TPOC. The DHS TPOC name, address, and contact information will be provided at award.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a PNR (**Section J, Attachment Q**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Appointment Letter (**Section J, Attachment A**). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Mr. William Moore
GSA FAS AAS Region 8 (8QFA)
One Denver Federal Center
P.O. Box 25526 Building 41
Denver, CO 80225
Telephone (Mobile): (b) (6)
Email: will.moore@gsa.gov

Contracting Officer's Representative:

Technical Point of Contact:

TPOC: Colleen McDarby
Telephone: (202) 878-2765
Email: (b) (7)(C)

Alternate Technical Point of Contact:

ATPOC: Niki Lane
Telephone: (202) 368-8374
Email: (b) (7)(C)

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009) to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: *(from GSA Form 300, Block 2)*

Paying Number: *(ACT/DAC NO.) (from GSA Form 300, Block 4)*

FEDSIM Project Number: HS00860

Project Title: CDM DEFEND Group D

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category, supporting documentation for completed travel, and fully executed Material Inspection and Receiving Reports (Form DD250) (**Section J, Attachment N**).

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Tracking and Ordering System (TOS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in TOS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. The Assisted Acquisition Services Business Systems (AASBS) Help Desk should be contacted for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice to the FEDSIM COR and DHS TPOC for review prior to its submission to GSA. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. The contractor shall submit simultaneous copies of the invoice to both GSA and the DHS TPOC. Receipts are provided on an as-requested basis.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

a. Governmentwide Acquisition Contract (GWAC) Contract Number
b. TO Award Number (NOT the Solicitation Number)
c. Contractor Invoice Number
d. Contractor Name
e. POC Information
f. Current POP
g. Amount of invoice that was subcontracted
h. Amount of the invoice that was subcontracted to a small business must be made available upon request

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the POP covered by the invoice (all current charges shall be within the active POP) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in **Section B**), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee company
c. Exempt or non-exempt designation
d. Employee Alliant labor category
e. Current monthly and total cumulative hours worked
f. Direct Labor Rate
g. Corresponding proposed labor rate
h. Effective hourly rate (e.g., cumulative costs/cumulative hours)
i. Current approved billing rates in support of costs billed
j. Itemization of cost centers applied to each individual invoiced
k. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable))
l. Any cost incurred not billed by CLIN (e.g., lagging costs)
m. Labor adjustments (from any previous months (e.g., timesheet corrections))
n. Associated CTN and RFS number, if applicable

All cost presentations provided by the contractor in MS Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP (**Section J, Attachment E**) for additional information on the award fee determination process.

G.3.2 TOOLS AND OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the POP covered by the invoice and the CLIN number and title. In addition, the contractor shall provide supporting documentation including fully executed Material Inspection and Receiving Reports (Form DD250) (**Section J, Attachment N**) and the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased
b. RIP Number
c. RFS Number
d. Date RIP accepted by the Government

e. Date received by Receiving Agency
f. Associated CLIN
g. Project-to-date totals by CLIN
h. Cost incurred not billed by CLIN
i. Remaining balance of the CLIN, identified by CTN and RFS if applicable

All cost presentations provided by the contractor shall also include OH charges, G&A charges and Fee in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous United States (U.S.).
b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR. The invoice shall include the POP covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. TAR number or identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Number of days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs
j. Total charges
k. Explanation of variances exceeding ten percent of the approved versus actual costs
l. Indirect handling rate

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's DCAA cost disclosure statement.

G.4 TASK ORDER CLOSEOUT

The Government will unilaterally close out the TO NLT six years after the end of the TO POP if the contractor does not provide final DCAA rates by that time.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government will evaluate additional Key Personnel as proposed by the contractor.

a. Project Manager (PM)
b. Lead Systems Integration Manager
c. Cyber Architect

The Government desires that Key Personnel be assigned for the duration of the TO. Key Personnel may be replaced or removed subject to **Section H.1.4** Key Personnel Substitution.

It is desirable for the contractor to achieve efficiencies in the composition of its proposed staffing. Although Key Personnel shall be available to support this TO at all times (assigned for the duration of the TO), full-time commitment by Key Personnel is not mandatory. Efficiencies may be achieved, for example, by sharing Key Personnel and/or non-Key Personnel across multiple Agencies and TOs.

H.1.1 PROJECT MANAGER (PM)

The contractor shall identify a PM to serve as the Government's main POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM shall ultimately be responsible for the quality and efficiency of the TO. The PM shall have organizational authority to execute the requirements of the TO. The PM shall assign tasking to contractor personnel, supervise ongoing technical efforts, and manage overall TO performance to ensure the optimal use of assigned resources and subcontractors. This Key Person shall have the ultimate authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. The PM shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual and programmatic issues.

It is required that the PM has the following qualification:

a. Be an employee of the prime contractor at the time of proposal submission.
b. Possess a TS security clearance and be Sensitive Compartmented Information (SCI) eligible.

It is desirable that the PM has the following qualifications:

a. Demonstrated competencies shown with the following:
    1. Experience in completing, leading, or directing the work of others on projects similar to the size, scope, and complexity of the work and environment described in **Section C**.
    2. Managerial experience providing technical advice, organizing, planning, directing, and managing staff to ensure goals and objectives are achieved.
    3. Experience with the management and supervision of teams comprised of multi-disciplinary employees.

4. Experience with risk management, issue resolution, problem solving, and customer service.
5. Experience managing teams working on system architectures, networks, and operations.

b. Current Project Management Institute (PMI) Project Management Professional or Program Management Professional (PgMP) certification.
c. A minimum of 15 years of experience managing complex, heterogeneous enterprise security integration projects across multiple disciplines for U.S. Government Agencies.
d. A minimum of five years of experience as a Systems Engineer or Systems Architect, preferably for a U.S. Government Agency.

H.1.2 LEAD SYSTEMS INTEGRATION MANAGER

It is desirable that the Lead Systems Integration Manager has the following qualifications:

a. Current Certified Information Systems Security Professional (CISSP) certification.
b. A minimum of eight years of experience managing integration teams similar to the size, scope, and complexity of the work and environment described in **Section C**.
c. Experience implementing IT security projects in complex and heterogeneous environments, including the following:
    1. Experience developing, configuring, and delivering COTS software in support of enterprise security solutions.
    2. Experience leading integration planning activities of multiple U.S. Government Agencies on a scale similar to this TO.
    3. Experience leading multi-organizational and matrixed technical resources and teams in accordance with approved integration plans and TO terms and conditions.
d. A minimum of six years of experience managing technical integration and solution delivery issues.
e. A minimum of four years of IT security operational experience, including assessment of information assurance and interoperability.
f. Demonstrated expertise in security policy and implementation.
g. Experience developing and integrating Continuous Monitoring capabilities.
h. Possess a TS security clearance and be SCI eligible.

H.1.3 CYBER ARCHITECT

It is desirable that the Cyber Architect has the following qualifications:

a. A minimum of ten years of experience managing cyber architecture teams on projects similar to the size, scope, and complexity of the work and environment described in **Section C**.
b. Experience developing cybersecurity solutions across a diverse and heterogeneous IT environment, including the following:
    1. Technical leadership in Enterprise Architecture (EA), Service-Oriented Architecture (SOA), and IT Service Delivery to multiple U.S. Government Agencies.

2. Demonstrated experience in security solution design using existing and emerging technologies to achieve enterprise solutions.

c. A minimum of six years of experience working with Security Authorization requirements, developing and enhancing the security risk posture, and analysis and reporting of IT security metrics.

d. A minimum of four years of experience in security policy and emerging cybersecurity technologies.

e. Possess a TS security clearance and be SCI eligible.

H.1.4 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to using other than personnel specified in proposals in response to a TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR. This notification shall be NLT ten calendar days in advance of any proposed substitution and shall include justification (including Key Personnel Qualification Matrix (KPQM) for the proposed substitution, resume(s), and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the person being substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed substitute person is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost-Reimbursement).

H.2 OTHER DESIRABLE SKILLS

The Government does not intend to dictate the composition of the ideal team; therefore, contractors may propose additional Key Personnel. It is desirable for the contractor to propose Key Personnel that possess the skills/qualifications listed in **Section J, Attachment S**.

H.3 GOVERNMENT-FURNISHED PROPERTY (GFP)

As defined in FAR 52.245-1 (representing content as prescribed in FAR Part 45.107(a)(1)):

All contractors employees furnished with GFP shall ensure Government barcodes are not removed. In all GFP cases, the Government retains title to the property. It is the contractor's responsibility to use GFP as it was authorized, and for the purpose intended. In the event the contractor uses Government property for other purposes without written authorization from the FEDSIM CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs. The contractor shall be directly responsible and accountable for all contract property in its possession in accordance with the requirements of the TO; this also includes any contract property in the possession or control of a subcontractor.

H.4 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide access to its IT systems, with which the contractor shall integrate its technical solution, as well as the Federal Dashboard after it has been implemented.

Information about the Agency IT/Network environments and systems will be provided as GFI at TOA.

The contractor shall protect all GFI (e.g., Government data) by treating the information as Sensitive But Unclassified (SBU). SBU information and data shall only be disclosed to authorized-personnel as described in the TO herein. The contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards.

When no longer required, this information and data shall be returned to Government control, destroyed, or held until otherwise directed by the FEDSIM CO. The contractor shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

If work under this TO requires that the contractor's personnel have access to Privacy Information, contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable Agency rules and regulations.

H.5 SECURITY REQUIREMENTS

The Government requires all information pertaining to this TO be stored and protected in accordance with Government policy regarding SBU information. Therefore, no information shall be stored or transmitted outside the U.S. The information associated with this TO is critical infrastructure information as defined by 1016(e) of the U.S. Patriot Act of 2001 (42 U.S.C. 5195c(e)).

DHS security requirements are also applicable to this TO. In some instances, the contractor shall have to follow specific Agency security requirements that will be provided post-award as GFI. For work that does not require contractor to access DHS networks or IT resources, the contractor shall defer to the Agency-specific Entrance on Duty (EOD) processes.

H.5.1 FACILITY CLEARANCE LEVEL (FCL)

At the time of proposal submittal, the contractor shall have a contractor facility with an approved facility clearance at the TS level. Although the TO utilizes information at the SBU level, the FCL will allow for greater classification levels as directed by the Government, such as through an RFS.

An FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the Confidential, Secret, or TS level. The FCL includes the execution of a DoD Security Agreement (DD Form 441 and DD Form 441-1) and Certificate Pertaining to Foreign Interests (Standard Form (SF) 328). Under the terms of an FCL agreement, the Government agrees to issue the FCL and inform the contractor as to the security classification of information to which the contractor will have access. The contractor, in turn, agrees to abide by the security requirements set forth in the National Industrial Security Program Operating Manual (NISPOM).

The Government will submit a DoD Contract Security Classification Specification (**Section J, Attachment U**) for the TS level post-award.

In general, all necessary FCLs shall be at the expense of the contractor.

H.5.2 PERSONNEL SECURITY CLEARANCES

At the time of solicitation release, the planned work is at an unclassified level. Each RFS will document any security clearance requirements as applicable.

In general, all necessary employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

H.5.3 DHS CONTRACTOR SECURITY REQUIREMENTS

H.5.3.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12)

The contractor shall provide a list of contractor personnel that require DHS badges and security clearances. The Government will process background investigation and/or security clearances for the contractor staff to occur after submission of the staff listing, provided the individuals meet the necessary security qualifications.

H.5.3.2 POST-AWARD SECURITY REQUIREMENTS

Contractors requiring access to DHS systems (to include DHS GFP or CDM Agency/Federal Dashboard) require personnel security vetting, to include the scheduling and adjudication of the appropriate level of background investigation processed by the DHS Personnel Security Division. The DHS CDM PMO, in conjunction with the DHS Personnel Security Division, shall have and exercise full control over granting, denying, withholding, or terminating unescorted Government facility and/or SBU Government information access for contractor employees, based upon the results of a background investigation. Contractor employees assigned to the TO not needing access to SBU Agency information or recurring access to Agency facilities shall not be subject to security suitability screening.

Contractor employees awaiting an EOD decision may begin work on the TO provided they do not access SBU Government information. Limited access to Government buildings may be allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, non-recurring meetings, and begin transition work.

The contractor shall further understand that it must propose employees whose background offers the best prospect of obtaining a security badge approval for access. Non-U.S. citizens (foreign nationals and/or dual citizenships) are not permitted under this TO.

H.5.3.3 CONTRACTOR FITNESS DETERMINATION

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Contractor employees under the TO, requiring access to sensitive information, shall be able to obtain “DHS Suitability.” The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security/PSD. Prospective contractor employees shall submit the following completed forms to the DHS Office of Security/PSD. The SF 85P shall be completed electronically, through the OPM’s Electronic Questionnaires for Investigations

Processing (e-QIP) System. The following completed forms shall be given to the DHS Office of Security/PSD no more than three days after TOA or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor:

a. Standard Form 85P, "Questionnaire for Public Trust Positions"
b. FD Form 258, "Fingerprint Card" (two copies)
c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon TOA.

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the Government do not relieve a contractor from performing under the terms of the TO.

DHS may, as it deems appropriate, authorize and grant a favorable EOD decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to Government facilities or information at any time during the term of the TO. No employee of the contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five days of occurrence. The contractor shall return to the CDM Customer Representative (CR) all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the CDM CR, referencing the pass or card number, name of individual to whom it was issued, and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel shall have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

DHS Security Office POC Information:

Office of Security/PSD
Customer Service Support
Washington, D.C. 20528

Telephone: (202) 447-5010

H.5.3.4 IT SECURITY TRAINING AND OVERSIGHT

All contractor employees accessing Government information systems, facilities, or data shall receive Security Awareness Training. This training will be provided by DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle SBU information within or under the supervision of the DHS shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS contractors with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems shall be continually monitored while performing these duties. The contractor's PM shall be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures shall be reported to the local Security Office or Information System Security Officer (ISSO).

Contractors who require access to Group D networks may also be required to complete Group D Agency-specific security awareness training.

H.5.3.5 SBU NETWORK SECURITY REQUIREMENTS

Contractor employees (to include applicants, temporaries, part-time, and replacement employees) under the TO, requiring access to SBU information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the TO. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective contractor employees shall submit the following completed forms to the DHS Security Office 30 days prior to EOD of any employees, whether a replacement, addition, or subcontractor employee:

a. Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
b. FD Form 258, "Fingerprint Card" (two copies)
c. DHS Form 11000-6 ,"Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

DHS will provide the required forms at TOA. Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon TOA. Be advised that unless an applicant requiring access to SBU information has resided in the U.S. for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

In addition, the contractor may be required to complete security access forms for each Agency on this TO. The issuance of network access forms will be completed after TOA.

H.5.3.6 INFORMATION ASSURANCE (IA)

This requirement implements the Government acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems to the extent that those requirements apply to the Group D Agencies and DHS. Contractor actions relating to information security must be in accordance with relevant Federal security statutes, regulations, guidance, and memoranda. These statutes, regulations, guidance, and memoranda include, but are not limited to, the following:

a. FISMA of 2002
b. HSPD-12
c. Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.)
d. Public Law 106--398, Section 1061
e. OMB Circular A-130, *Management of Federal Information Resource*
f. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
g. OMB M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
h. OMB M-07-18 *Implementation of Commonly Accepted Security Configurations for Windows*
i. Operating Systems (Federal Desktop Core Configuration)
j. Federal Server Core Configuration Standard
k. NIST SP to include the SP 800-18 *Guide for Developing Security Plans for Federal Information Systems*
l. NIST SP to include the SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems*
m. NIST SP to include the SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*
n. FIPS, to include, but not be limited to, FIPS 140-2 *Security Requirements for Cryptographic Modules*, 199, and 200

These requirements safeguard IT services provided to Agencies such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems. Along with these Federal requirements, any solution must comply with the standards detailed within the Agency Policies, which will be made available as needed. In addition to existing Federal standards and guidelines, it is the contractor's responsibility to adhere to new Federal standards/requirements that pertain to the security of unclassified information and information systems as these requirements are issued.

Information systems used or operated by the Agency or by a contractor of the Agency and DHS or other organization on behalf of the Agency must be authorized to operate by the Agency Authorizing Official (AO) through the certification and accreditation process as outlined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The certification process verifies that information systems have employed security controls consistent with the sensitivity of the information maintained by the system as defined by FIPS 199 and SP 800-53 and acceptably meets Federal standards such as the list of regulations

identified above. During the Certification and Accreditation (C&A) process, the contractor is required to work with the Government in good faith and without question or delay to ensure that adequate mechanisms are in-place and used to protect information produced, processed, stored, and/or transmitted on or by the application.

The contractor shall provide the Agency with all required documentation to support the Agency's security authorization, to include inputs to relevant portions of the Agency GSS SSP including descriptions of the management, operational, and technical security controls (as defined in NIST 800-53) employed in the system to the DHS TPOC and FEDSIM COR for Agency approval. This security documentation shall be prepared consistent in form and content with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and include any additions/augmentations described in Agency IT Policy. The security documentation shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The documentation shall be reviewed and updated in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* and FIPS 200 on an annual basis. Strict security requirements shall be imposed for work tasks that will be accomplished at the contractor facility which includes, but is not limited to, the following:

a. Making configuration changes to improve security (harden the application) and/or otherwise address/mitigate discovered security vulnerabilities.
b. Providing all requested information and resolve any information security vulnerabilities identified by the Agency IA Office and/or detailed in the Security Test and Evaluation Report and/or Risk Assessment Report.
c. Documenting all system configurations in the Standard Install Process (SIP).

All activities performed at contractor facilities shall comply with the following:

a. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems.*
b. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.*
c. NISPOM, DoD Manual, DoD 5220.22-M (when applicable).

The contractor shall not co-host Agency systems with third-party sites that contain inappropriate content, which may include, but is not limited to, pornography, gambling, and political views.

The contractor shall not use Agency equipment for activities that could be considered offensive or inappropriate, including activities that may:

a. Place undue burden on Agency system components and resources.
b. Involve fundraising, non-Agency commercial purposes, non-Agency profit activities, stock trades, and gambling.
c. Result in access or transmission of objectionable material.
d. Incur additional cost to the Agency.

In addition, webmail use on the Agency equipment is strictly prohibited.

H.5.4 SECURITY SAFEGUARDS

The details of any safeguards the contractor may design or develop under this TO are the property of the Government and shall not be published or disclosed in any manner without the FEDSIM CO's express written consent.

The details of any safeguards that may be revealed to the contractor by the Government in the course of performance under the TO shall not be published or disclosed in any manner without the FEDSIM CO's express written consent.

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the contractor shall afford the Government access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases in accordance with the FAR 52.239-1. The contractor shall use best efforts to ensure that the Government has similar access to the facilities, installations, technical capabilities, operations, documentation, records, and databases of its third-party hosting provider or sub-contractor.

If new or unanticipated IT security threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institutions of new safeguards, with final determination of appropriateness being made by the Government.

H.5.5 PRIVACY CONSIDERATIONS

The Government anticipates that this TO will not involve access to privacy information, including SPII. However, in the event that the TO results in contractor access to privacy information, then the following terms apply:

H.5.5.1 REQUIRED SECURITY AND PRIVACY TRAINING

The contractor shall provide training for all employees and subcontractors that have access to SPII as well as the creation, use, dissemination, and/or destruction of SPII, at the outset of the subcontractor's/employee's work on the TO and every year thereafter. Training shall include procedures on how to properly handle SPII, to include security requirements for transporting or transmitting SPII information, requirements for reporting a suspected breach or loss of SPII within one hour, and supporting privacy compliance and breach management activities. The contractor shall submit an email notification to the FEDSIM COR and DHS TPOC that all the contractor's employees have received privacy training prior to the beginning of the TO.

The privacy training can be obtained via Government-provided Compact Disc (CD) or through the Homeland Security Information Network at https://share.dhs.gov/nppdprivacy101training/. DHS has also published a guidebook defining SPII and setting standards for SPII handling and protection. The DHS Handbook for Safeguarding SPII is a 30-page public document on the DHS Privacy Office website.

http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

The Management Directive for "safeguarding of SBU information" and related policies require all individuals accessing NPPD information, regardless of their employment status, be they Federal or contractor employees, to take the Information Security and Records Management Training annually. Both courses (Information Security and Records Management) can be obtained via Government-provided CD. The contractor shall maintain copies of certificates as a record of compliance. The contractor shall submit an annual email notification to the FEDSIM COR and DHS TPOC that the required Information Security, Records Management, and Privacy training has been completed for all the contractor's employees.

H.5.5.2 SUSPECTED LOSS OR COMPROMISE OF SPII (BREACH)

The contractor shall report the suspected loss or compromise of SPII by its employees or subcontractors to the DHS Help Desk at 1-800-250-7911 within one hour of the initial discovery.

The contractor shall also notify the FEDSIM CO, FEDSIM COR, and DHS TPOC via the PNR of the suspected loss or compromise. As part of the PNR, the contractor shall develop and include an Incident Response Plan, an internal system by which its employees and subcontractors are trained to identify and report potential loss or compromise of SPII. The PNR shall also include a written report within 24 hours of the suspected loss or compromise of SPII containing the following information (the written report shall also be provided to the NPPD Office of Privacy at NPPDPrivacy@hq.dhs.gov):

a. Narrative, detailed description of the events surrounding the suspected loss/compromise.
b. Date, time, and location of the incident.
c. Type of information lost or compromised.
d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
e. Names of person(s) involved, including victim, contractor employee/subcontractor, and any witnesses.
f. Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed.
g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

Notwithstanding any other remedies available to NPPD, the contractor shall indemnify the NPPD against all liability (including costs and fees) for any damages arising out of violations of this requirement.

The contractor shall cooperate with NPPD or other Government Agency inquiries into the suspected loss or compromise of SPII to facilitate activities outlined in the DHS Privacy Incident Handling Guide (PIHG) and OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007. The DHS PIHG is an 88-page public document on the DHS Privacy Office website.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

At the Government's discretion, contractor employees or subcontractor employees may be identified as no longer eligible to access SPII or to work on that TO based on their actions related to the loss or compromise of SPII.

In the event that a SPII breach occurs as a result of the violation of a term of this TO by the contractor or its employees, the contractor shall, as directed by the FEDSIM CO and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor shall be responsible for reimbursing the Government for those expenses.

H.5.6 SECURITY COMPLIANCE REQUIREMENTS

H.5.6.1 COMPLIANCE WITH DHS SECURITY POLICY

All SBU systems employed by this TO must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A, *Sensitive Systems Handbook*. All contractor systems used to process sensitive DHS data must be accredited for that use.

All national security systems produced by or supported under this TO must be compliant with DHS 4300B, *DHS National Security System Policy*.

All DHS intelligence systems produced by or supported under this TO must be compliant with DHS 4300C, *DHS Sensitive Compartmented Information (SCI) Systems Policy Directive*.

H.5.6.2 ACCESS TO UNCLASSIFIED FACILITIES, INFORMATION TECHNOLOGY (IT) RESOURCES, AND SENSITIVE INFORMATION

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and TO performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle SBU information. DHS MD 4300.1, *Information Technology Systems Security,* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. The contractor shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all TOs that require access to DHS facilities, IT resources, or sensitive information. The contractor shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the TO.

H.5.6.3 SECURITY REVIEW

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this TO are being implemented and enforced. The contractor shall afford DHS, including the organization of DHS Office of the CIO, the Office of the Inspector General, authorized FEDSIM CO, FEDSIM COR, and other Government oversight organizations, access to the contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this TO. The contractor will contact the DHS CISO to coordinate and participate in the review and inspection activity of Government oversight organizations external

to DHS. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS and to preserve evidence of computer crime.

H.5.6.4 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY (IT) RESOURCES

All unclassified IT resources shall be managed and controlled in compliance with the Department of Homeland Security Acquisition Regulation (HSAR) clause 3004.470: Security requirements for access to unclassified facilities, information technology resources, and sensitive information.

H.5.6.5 CONTRACTOR EMPLOYEE ACCESS

All contractor employee access shall be managed and controlled in compliance with HSAR clause 3004.470: Security requirements for access to unclassified facilities, information technology resources and sensitive information.

H.6.4 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

H.6.4.1 CONTRACTOR SAFEGUARDS

The contractor shall support supply chain protections as defined in the NIST 800-53 SA-12 control, which states, "The organization protects against supply chain threats to the information system, system component, or information system service by employing (Assignment: organization-defined security safeguards) as part of a comprehensive, defense-in-breadth information security strategy." NIST 800-53 SA-12 can be located at the NIST website.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

The contractor shall provide the Government with an SCRM Plan (**Section F, Deliverable 54)** that describes what safeguards it intends for supply chain protections which could include only using signed software.

H.6.4.2 COMPANY INFORMATION REVIEW

For the purposes of supply chain risk assessment under this TO, the "organization-defined security safeguards" referenced above will include a Government CO's review of any negative findings reported by DHS as a result of the Company Information Review (CIR) conducted by DHS. The contractor is under a continuing obligation to ensure that all responses to the acquisition risk questions (**Section J, Attachment V**) answered in the CIR remain complete, accurate, and up-to-date. The contractor shall promptly notify and submit updated responses to the FEDSIM CO when any change in circumstances of the contractor or subcontractors warrants a change in the contractor's or subcontractor's responses to the acquisition risk questions. In addition, the contractor is under a continuing obligation to promptly disclose to the FEDSIM CO any proposed additional or replacement subcontractors.

H.7 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.7.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

b. The contractor is required to complete and sign an OCI Statement (**Section J, Attachment F**). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.

c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.

d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.

e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

H.7.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an Agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) form (**Section J, Attachment C**) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Execute and submit an Addendum to Corporate NDA (**Section J, Attachment D**) prior to the commencement of any work on the TO.

b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or quote information, or source selection information.

c. Are instructed in Far Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel also must be listed on a signed Addendum to Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided

by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.8 INFORMATION TECHNOLOGY (IT) ACCESSIBILITY FOR PERSONS WITH DISABILITIES

H.8.1 SECTION 508 COMPLIANCE REQUIREMENTS

a. Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220), requires that when Federal agencies develop, procure, maintain, or use Information and Communications Technology (ICT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All ICT that is procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS shall comply with the applicable technical and functional performance criteria of the Section 508 standards unless a general exception applies.

b. When modifying commercially available or Government-owned ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance.

c. When providing and managing hosting services for ICT items, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance prior to providing the hosting service.

d. When providing installation, configuration, or integration services for ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

e. When providing maintenance upgrades, substitutions, and replacements to ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to upgrade, substitution, or replacement.

f. When procuring ICT and where products that fully conform to the Section 508 standards are not commercially available, the contractor shall procure the ICT that best meets the Section 508 standards consistent with the Agency's business needs (1194, 202.7 Best Meets). When applying this standard, all procurements of ICT shall have documentation of market research that identifies which provisions cannot be met by commercially available items, and the basis for determining that the ICT to be procured best meets the Standards consistent with meeting Agency business needs as required by FAR 39.2. Any selection of a product or service that does not best meet the Revised 508 Standards due to a significant difficulty or expense shall only be permitted under an Undue Burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 139-05.

H.8.2 SECTION 508 ACCESSIBILITY STANDARDS

Revised 508 Standards: Applies to any component or portion of existing ICT purchased, developed, or altered on or after January 18, 2018, under this PWS.Text of the standards and guidelines can be found at the United States Access Board website.

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines

Chapter 2: Scoping Requirements. Applies to all ICT procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS.

Chapter 3: Functional Performance Criteria. Applies to all web- and non-web-based software procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS that does not fully conform to Chapter 5: Software Technical Standards.

Chapter 4: Hardware Technical Standards. Applies to all hardware procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS.

Chapter 5: Software Technical Standards. Applies to all web- and non-web-based software procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS.

Chapter 6: Support Documentation & Services Technical Standards. Applies to all support documentation and services under this PWS.

Original 508 Standards: Applies to any components or portion of existing ICT that has not been altered on or after January 18, 2018, under this PWS, and fully complies with the Original 508 Standards.

Section 508 Conformance Testing Methods: DHS testing methods used to validate web and non-web electronic content for conformance to the Section 508 Standards.

a. Web and Software: https://www.dhs.gov/compliance-test-processes

b. Electronic reports and documentation in MS Office or Adobe PDF format: https://www.dhs.gov/compliance-test-processes

H.8.3 SECTION 508 APPLICABLE EXCEPTIONS

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the FEDSIM COR and determination will be made in accordance with DHS MD 139-05. DHS has identified the following exceptions that may apply: E202.4 Federal Contracts, all ICT that is exclusively owned and used by the contractor to fulfill this work statement does not require conformance with the Section 508 standards. This exception does not apply to any ICT deliverable, service, or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this PWS and, for the purposes of this requirement, are not considered members of the public.

H.8.4 ACCEPTANCE CRITERIA

Prior to acceptance of ICT items that are developed, modified, or configured subject to this contract, the Government reserves the right to require the contractor to provide the following:

a. Accessibility test results based on the required test methods.
b. Documentation of features provided to help achieve accessibility and usability for people with disabilities.
c. Documentation of core functions that cannot be accessed by persons with disabilities.
d. Documentation on how to configure and install the ICT Item to support accessibility.
e. Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).

H.9 ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire POP and shall permit timely development of all necessary cost data in the form required by the contract.

H.10 APPROVED PURCHASING SYSTEM

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

H.11 TRAVEL

H.11.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. JTR Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.11.2 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel coordinated with the DHS TPOC and approved by the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR (**Section J, Attachment O**) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR and DSSR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose, including the RFS number (if applicable).
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.12 TOOLS (HARDWARE/SOFTWARE) AND/OR OTHER DIRECT COSTS (ODCs)

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will either be identified at the time a TOR is issued or may be identified during the course of the TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR and DHS TPOC a RIP (**Section J, Attachment K**). If the contractor is to lose an approved purchasing system at any time during TO performance (due to a temporary suspension of the Alliant Prime contractor's purchasing system after TOA), the contractor shall submit to the FEDSIM CO a Consent to Purchase (CTP) (**Section J, Attachment L**) until such time that the purchasing system suspension has been lifted. Failure to possess a Government-approved purchasing system for an extended period of time after award may be grounds for contractor default. The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. Where applicable, the GSA IT Schedule 70 CDM Tool SIN cost should be used as one of the cost comparisons. The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.14.2.

When the contractor submits the RIP or CTP, it shall also submit the following, when applicable:

a. A Form DD1149 (**Section J, Attachment M**) for each group of tools, as identified by manufacturer and/or receiving Agency, that has been reviewed and signed by the receiving Agency to show concurrence.
b. A Form DD250 (**Section J, Attachment N**) to match each Form DD1149 to be used upon delivery of tools as confirmation of receipt.

The contractor shall deliver the Form DD250s to the receiving Agency along with the tools/ODCs. The receiving Agency POC will review the delivery for accuracy and show acceptance through signature on the DD250. The contractor shall email the signed DD250s to the FEDSIM COR for approval. Invoicing for procurements must have associated DD250s with the FEDSIM COR signature as supporting documentation.

H.12.1 TOOLS

Tools can be either specific to a CDM capability or ancillary. Tools that are specific to CDM capabilities (CDM tools) are identified on the CDM APL. Information on the CDM APL can be found at http://www.gsa.gov/CDM.

If a tool specific to a CDM capability is identified as necessary to support the TO but is not on the APL, the contractor can request through the CDM APL Product Submission Instructions to add a tool. The DHS CDM PMO will make the determination for accepting the tool as part of the review and submission process.

H.13 ENTERPRISE ARCHITECTURE (EA) COMPLIANCE TERMS AND CONDITIONS

All DHS-funded solutions and services shall meet DHS Enterprise Architecture (EA) (referred to as Homeland Security (HLS) EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

a. All developed solutions and requirements shall be compliant with the HLS EA.
b. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
c. Description information for all data assets, information exchanges, and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
d. Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01, and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
e. Applicability of Internet Protocol Version 6 (IPv6) to Hosts, Routers, Systems (HRS)-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile NIST SP 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

H.14 COMMERCIAL SUPPLIER AGREEMENTS

H.14.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in **Section C** and as contemplated in the Tools and ODC CLINs in **Section B.4** (included with the final TOR) may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic

or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). For purposes of this TO, the Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14.

H.14.2 Unless otherwise agreed by the Parties in a specific purchase order, the end user license agreement, terms of service, or comparable end user authorization will allow the licensed software and services to be used as described in its documentation. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government in negotiating suitable terms to comply with this Section which shall be “other rights and limitations” pursuant to FAR clause 52.227-14 (d), Rights In Data – General (May 2014), Alternate III (Dec 2007).

Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following:

(a) subject to purchase of applicable licenses, access and use by contractors acting on behalf of the Ordering Entity solely for Ordering Entity business purposes during the term of the applicable Supplier Agreement ;

(b) in the event of a cybersecurity incident or breach reported by the Ordering Entity or Contractor, access and use by employees of other Federal, state, and local law enforcement agencies acting on behalf of Ordering Entity solely for Ordering Entity business purposes in responding to the cybersecurity incident or breach;

(c) to the extent applicable to the licensed software, transfer to a different data center and/or a successor contractor’s cloud in each case solely for Ordering Entity business purposes and in accordance with all other license terms and ;

(d) development of intellectual property works using Supplier’s licensed application program interfaces (APIs) in accordance with applicable license terms is permissible for the Ordering Entity or a contractor (i) acting on its behalf using government funds solely for Ordering Entity business purposes.

H.15 PRESS RELEASE

The contractor shall not make any press releases pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.16 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.17 NEW SOFTWARE

H.17.1 RIGHTS IN NEW CODE

Notwithstanding the foregoing in **Section F.3.1**, Source, Object Executable and Run-Time Code, in order to ensure that the commercial software products and open source tools purchased or provided by the contractor under this TO meet the Government's needs, the contractor shall ensure that all associated Software Agreements permit the creation of new code and customizations and their delivery to the Government as and when required by the Government; vest the data rights to the new code and customizations exclusively in the Government; and do not restrict Government's right and ability, directly or indirectly, to use any and all versions of the new code and customizations installed at a Government facility and to further develop and distribute them, with no further royalties or other payments being due to the contractor or any other party. If the rights to the new code and customizations are not vested in the Government upon their creation, the contractor shall assign copyright in the new code and customizations to the Government as contemplated under the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007) upon delivery in accordance with **Section F.3**.

H.17.2 DEFERRED ORDERING OF TECHNICAL DATA OR COMPUTER SOFTWARE

In addition to technical data or computer software specified elsewhere in this TO to be delivered hereunder, the Government may, at any time during the performance of this TO, or within a period of three years after acceptance of all items (other than technical data or computer software) to be delivered under this TO or the termination of this TO, order any technical data or computer software generated in the performance of this TO or any subcontract hereunder. When the technical data or computer software is ordered, the contractor shall be compensated for converting the data or computer software into the prescribed form for reproduction and delivery.

The obligation to deliver the technical data of a subcontractor and pertaining to an item obtained from the contractor shall expire three years after the date the contractor accepts the last delivery of that item from that subcontractor under this TO. The Government's rights to use said data or computer software shall be pursuant to the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007) and the clauses listed in **Section H.17.3**, Rights in Technical Data and Computer Software Developed Exclusively at Private Expense, of this TO.

H.17.3 RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE DEVELOPED EXCLUSIVELY AT PRIVATE EXPENSE

(a) For the purposes of rights in data in the operation of this TO, the definitions, the treatment of unauthorized data markings, and the treatment of omitted markings shall be in accordance with paragraphs (a), (e), and (f), respectively, of the clause at FAR 52.227-14 in effect on the date of TOA.

(b) To the extent that the deliverables under this TO are authorized by the Statement of Work (SOW) to contain either technical data or computer software developed exclusively at private expense, those data shall be subject to the Government's rights below for the specific category of data and shall be marked only in accordance with the following terms:

(1) Limited Rights Technical Data. This TO may identify and specify the delivery of limited rights data, or the CO may require by written request the delivery of limited rights data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the contractor shall affix the following "Limited Rights Notice" to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of the clause at FAR 52.227-14 in effect on the date of TOA, in accordance with the notice:

Limited Rights Notice

(a) These data are submitted with limited rights under Government Task Order No. _____ (and subcontract _____, if appropriate). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure:

(1) Use (except for manufacture) by support service contractors.

(2) Evaluation by non-Government evaluators.

(3) Use (except for manufacture) by other contractors participating in the Government's program of which the specific TO is a part.

(4) Emergency repair or overhaul work.

(5) Release to a foreign Government, or its instrumentalities, if required to serve the interests of the U.S. Government, for information or evaluation, or for emergency repair or overhaul work by the foreign Government.

(b) This Notice shall be marked on any reproduction of these data, in whole or in part.

(2) Restricted Computer Software.

(i) This TO may identify and specify the delivery of restricted computer software, or the CO may require by written request the delivery of restricted computer software that has been withheld or would otherwise be entitled to be withheld. If delivery of that computer software is required, the Contractor shall affix the following "Restricted Rights Notice" to the computer software and the Government will treat the computer software, subject to paragraphs (e) and (f) of the clause at FAR 52.227-14 in effect on the date of TOA, in accordance with the notice:

Restricted Rights Notice

(a) This computer software is submitted with restricted rights under Government Task Order No. _____ (and subcontract _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this notice or as otherwise expressly stated in the Task Order.

(b) This computer software may be—

(1) Used or copied for use in or with the computer(s) for which it was acquired, including use at any Government installation to which such computer(s) may be transferred;

(2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

(3) Reproduced for safekeeping (archives) or backup purposes;

(4) Modified, adapted, or combined with other computer software, provided that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights;

(5) Disclosed to and reproduced for use by support service contractors or their subcontractors in accordance with paragraphs (b)(1) through (4) of this notice; and

(6) Used or copied for use in or transferred to a replacement computer.

(c) Notwithstanding the foregoing, if this computer software is copyrighted computer software, it is licensed to the Government with the minimum rights set forth in paragraph (b) of this notice.

(d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the TO.

(e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

(End of notice)

(ii) Where it is impractical to include the Restricted Rights Notice on restricted computer software, the following short-form Notice may be used instead:

Restricted Rights Notice Short Form

Use, reproduction, or disclosure is subject to restrictions set forth in TO No. _____ (and subcontract, if appropriate) with _____ (name of Contractor and subcontractor).

(End of notice)

(iii) If restricted computer software is delivered with the copyright notice of 17 U.S.C. 401, it will be presumed to be licensed to the Government without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

(End of Clause)

H.18 AWARD FEE

See the AFDP in **Section J, Attachment E**.

H.19 STANDARDS OF CONDUCT AND RESTRICTIONS

The contractor shall conform to standards of conduct, which include the following:

a. The contractor's employees shall dress appropriately for a professional office environment while at a Government facility.
b. Contractor employees shall only conduct official business directly related to the TO while performing work under the TO.
c. Use of GFP or records for company or personal use is strictly prohibited. For example, use of Government telephones to make personal phone calls at the Government's expense is prohibited.
d. The contractor is responsible for ensuring compliance with all laws, rules, and regulations governing conduct with respect to health, safety, and use of Government property. This

relates not only to the health and safety of contractor employees, but also to that of Government personnel and other individuals.

e. Contractor employees are expected to adhere to the high professional ethical standards to which Government personnel in a comparable position would be expected to adhere. In addition, contractor employees must comply with the pertinent provisions of the Office of Federal Procurement Policy Act Amendments of 1989 and 41 U.S.C. 423.

f. The contractor shall be responsible for the actions of all personnel provided to work under this TO. In the event that damages arise from work performed by contractor-provided personnel, under the auspices of this TO, the contractor shall be responsible for all resources necessary to remedy the incident.

H.20 CONTRACTOR'S BUSINESS CONFIDENTIAL OR FINANCIAL DATA

To the extent the work under this TO requires access to business confidential or financial data of other contractors, the contractor and its employees shall protect such data from unauthorized use and disclosure and agrees not to copy or use it for any purpose other than the performance of this TO. This data may be in various forms such as documents, raw photographic prints, computer printouts, or it may be interpretative results derived from analysis, investigation, or study efforts.

The contractor shall establish policies and procedures to implement the substance of this requirement at the individual employee and subcontracting level, which will ensure that contractor, teaming partner's and subcontractor's employees are made aware of the provisions and the contractor's implementing policies and procedures. Particular attention shall be given to keeping employees advised of the statutes and regulations applicable to the handling of other contractor's confidential business or financial data, in accordance with the FAR 9.505-4.

H.21 ASSOCIATE CONTRACTOR AGREEMENT (ACA)

The contractor shall establish an Associate Contractor Agreement (ACA) (**Section J, Attachment AB**) with the CDM Dashboard Provider which defines the roles and responsibilities for the Agency CDM Dashboard provided by the CDM Dashboard Provider. This agreement shall include the cooperative co-maintenance of the CDM Dashboard solution.

The contractor shall also establish ACAs with the PRIVMGMT Provider and the CREDMGMT Provider to define the roles and responsibility for transition out of those providers.

I.1 TASK ORDER CLAUSES

All applicable and required provisions/clauses set forth in FAR 52.301automatically flow down to all Alliant TOs, based on their specific contract type, PWS, competition requirements, commercial or not commercial, and dollar value as of the date the TO is issued.

I.1.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the FEDSIM CO will make their full text available. Also, the full text of a provision may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-14	Display of Hotline Poster(s)	OCT 2015
52.204-2	Security Requirements	AUG 1996
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other than Certified Cost or Pricing Data – Modifications	OCT 2010
52.216-7	Allowable Cost and Payment	JUN 2013
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data – General Alternate II and III	DEC 2007
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.227-21	Technical Data Declaration Revision and Withholding of Payment – Major Systems	MAY 2014
52.232-22	Limitation of Funds	APR 1985
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.239-1	Privacy or Security Safeguards	AUG 1996
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.247-14	Contractor Responsibility for Receipt of Shipment	APR 1984

FAR	TITLE	DATE
52.251-1	Government Supply Sources	APR 2012

I.1.2 FAR CLAUSES INCORPORATED BY FULL TEXT

52.204-23-Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

(a) Definitions. As used in this clause--

Covered article means any hardware, software, or service that--

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed

in whole or in part by a covered entity.

Covered entity means--

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from--

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) Reporting requirement. (1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the

website at https://dibnet.dod.mil/. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil/.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILANCE SERVICES OR EQUIPMENT (AUG 2019)

(a) *Definitions.* As used in this clause—

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably

believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a

subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the contractor within 30 days of the end of the period of performance.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the contractor within 30 days; provided that the Government gives the contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b. If the Government exercises this option, the extended contract shall be considered to include this option clause.

c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 69 months.

(End of clause)

52.247-67 SUBMISSION OF TRANSPORTATION DOCUMENTS FOR AUDIT (FEB 2006)

a. The Contractor shall submit to the address identified below, for prepayment audit, transportation documents on which the United States will assume freight charges that were paid –

1. By the Contractor under a cost-reimbursement contract; and
2. By a first-tier subcontractor under a cost-reimbursement subcontract thereunder.

b. Cost-reimbursement Contractors shall only submit for audit those bills of lading with freight shipment charges exceeding $100. Bills under $100 shall be retained on-site by the Contractor and made available for on-site audits. This exception only applies to freight shipment bills and is not intended to apply to bills and invoices for any other transportation services.

c. Contractors shall submit the above referenced transportation documents to the COR specified in **Section G**.

(End of clause)

I.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.212-71	Contract Terms and Conditions Applicable to GSA Acquisition of Commercial Items	JUN 2016
552.232.25	Prompt Payment	NOV 2009
552.239-70	Information Technology Security Plan and Security Authorization	JUN 2011
552.239-71	Security Requirements for Unclassified Information Technology Resources	JAN 2012

I.2.1 GSAM CLAUSES INCORPORATED BY FULL TEXT

552.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (FAR DEVIATION) (JULY 2015)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any commercial supplier agreement (as defined in 502.101) that includes any language, provision, or clause requiring the Government to indemnify the

Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such language, provision, or clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

552.232-78 COMMERCIAL SUPPLIER AGREEMENTS – UNENFORCEABLE CLAUSES (JULY 2015)

(a) When any supply or service acquired under this contract is subject to a commercial supplier agreement, the following language shall be deemed incorporated into the commercial supplier agreement. As used herein, "this agreement" means the commercial supplier agreement:

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) *Applicability*. This agreement is part of a contract between the commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license (including all contracts, task orders, and delivery orders not using FAR Part 12).

(ii) *End user*. This agreement shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) *Law and disputes*. This agreement is governed by Federal law. (A) Any language purporting to subject the U.S. Government to the laws of a U.S. state, U.S. territory, district, or municipality, or foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted. (B) Any language requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted. (C) Any language prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted.

(iv) *Continued performance*. If the supplier or licensor believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract

Disputes Act or other applicable Federal statute while continuing performance as set forth in 52.233-1 Disputes.

(v) *Arbitration; equitable or injunctive relief*. In the event of a claim or dispute arising under or relating to this agreement, (A) binding arbitration shall not be used unless specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the U.S. Government only when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act).

(vi) *Additional terms*.

(A) This commercial supplier agreement may unilaterally incorporate additional terms by reference. Terms may be included by reference using electronic means (e.g., via web links, click and accept, etc.). Such terms shall be enforceable only to the extent that:

(1) When included by reference using electronic means, the terms are readily available at referenced locations; and

(2) Terms do not materially change government obligations; and

(3) Terms do not increase government prices; and

(4) Terms do not decrease overall level of service; and

(5) Terms do not limit any other Government right addressed elsewhere in this contract.

(B) The order of precedence clause of this contract notwithstanding, any software license terms unilaterally revised subsequent to award that is inconsistent with any material term or provision of this contract is not enforceable against the government.

(vii) *No automatic renewals*. If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express Government approval.

(viii) *Indemnification*. Any clause of this agreement requiring the commercial supplier or licensor to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(ix) *Audits*. Any clause of this agreement permitting the commercial supplier or licensor to audit the end user's compliance with this agreement is hereby amended as follows: (A) Discrepancies found in an audit may result in a charge by the commercial supplier or licensor to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order. (B) This charge, if disputed by the ordering activity, will be resolved through the Disputes clause at 52.233-1; no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process. (C) Any audit requested by the

contractor will be performed at the contractor's expense, without reimbursement by the Government.

(x) *Taxes or surcharges*. Any taxes or surcharges which the commercial supplier or licensor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract or order and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xi) *Non-assignment*. This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under the clause at 52.232-23, Assignment of Claims.

(xii) *Confidential information*. If this agreement includes a confidentiality clause, such clause is hereby amended to state that neither the agreement nor the Federal Supply Schedule price list shall be deemed "confidential information." Issues regarding release of "unit pricing" will be resolved consistent with the Freedom of Information Act. Notwithstanding anything in this agreement to the contrary, the Government may retain any confidential information as required by law, regulation or its internal document retention procedures for legal, regulatory or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this agreement.

(2) If any provision of this agreement conflicts or is inconsistent with the preceding subparagraph (a)(1), the provisions of subparagraph (a)(1) shall prevail to the extent of such inconsistency.

(End of clause)

I.3 DHS HSAR CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at HSAR website:

https://www.dhs.gov/publication/archived-homeland-security-acquisition-regulation

HSAR	TITLE	DATE
HSAR Class Deviation 15-01	Safeguarding of Sensitive Information	MAR 2015

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically at the end of the TOR.

ATTACHMENT	TITLE
A	COR Appointment Letter
B	Acronym List
C	Corporate Non-Disclosure Agreement (NDA)
D	Addendum to Corporate NDA revised 3/19/2019
E	Award Fee Determination Plan (AFDP) entitled "DEFEND D Updated AFDP Period 3 6Aug19-31Jan20 Final 121719"
F	Organizational Conflict of Interest Statement
G	Incremental Funding Chart (electronically attached .xls)
H	Monthly Status Report (MSR) Template
I	DHS CDM TEMP
J	Procurement Report Template
K	Request to Initiate Purchase (RIP) Template revised 1/31/2019
L	Consent to Purchase (CTP)
M	Requisition and Invoice/Shipping Document (Form DD1149)
N	Material Inspection and Receiving Report (Form DD250)
O	Travel Authorization Request (TAR) (electronically attached .xls) revised March 25, 2019
P	Trip Report Template
Q	Problem Notification Report (PNR)
R.1	Reserved
R.2	Reserved
S	Key/Non-Key Personnel Desirable Skills and Qualifications
T	Deliverable Acceptance-Rejection Report
U	DoD Contract Security Classification Specification (DD Form 254) dated August 24, 2018
V	Acquisition Risk Questionnaire
W	DHS CDM IV&V Strategy Document
X	DHS SELC Process Overview
Y.1	CDM Technical Capabilities Requirements Document Volumes 1
Y.2	CDM Technical Capabilities Requirements Document Volumes 2
Z	Reserved
AA	Reserved
AB	Reserved
AC	Reserved
AD	Reserved

ATTACHMENT	TITLE
AE	Reserved
AF	Reserved
AG	Reserved
AH.1	Reserved
AH.2	Reserved
AH.3	Reserved
AH.4	Reserved
AI	RFS Tracking Table